WO02100037

Publication Title:

APPARATUS AND METHOD OF FLEXIBLE AND COMMON IPMP SYSTEM FOR PROVIDING AND PROTECTING CONTENT

Abstract:

Abstract of WO02100037

An apparatus of a flexible and common IPMP (intellectual property management and protection) system gives acquiring and mutual operability to the system by fetching a complete IPMP tool list held by a content stream or downloaded from the URL position. The apparatus provides an IPMP tool manager of a conforming IPMP terminal functioning as a pre-processing module, syntactically analyzes the IPMP tool list, and acquires an IPMP tool according to the IPMP tool ID, a position identifier related to it, and the IPMP tool format ID. By pre-compiling the IPMP tool into a binary format, the IPMP tool can be transferred or downloaded to the IPMP terminal, and a different binary format is prepared by a content provider for an object on a different platform of the IPMP terminal.

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2002 年12 月12 日 (12.12.2002)

PCT

(10) 国際公開番号
WO 02/100037 A1

(51) 国際特許分類[7]: H04L 9/14, G06F 17/60, G10L 19/00, H04N 7/08, 7/167

(21) 国際出願番号: PCT/JP02/05468

(22) 国際出願日: 2002 年6 月4 日 (04.06.2002)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2001-168259 2001 年6 月4 日 (04.06.2001) JP
特願2001-172451 2001 年6 月7 日 (07.06.2001) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府 門真市 大字門真１００６番地 Osaka (JP).

(72) 発明者; および

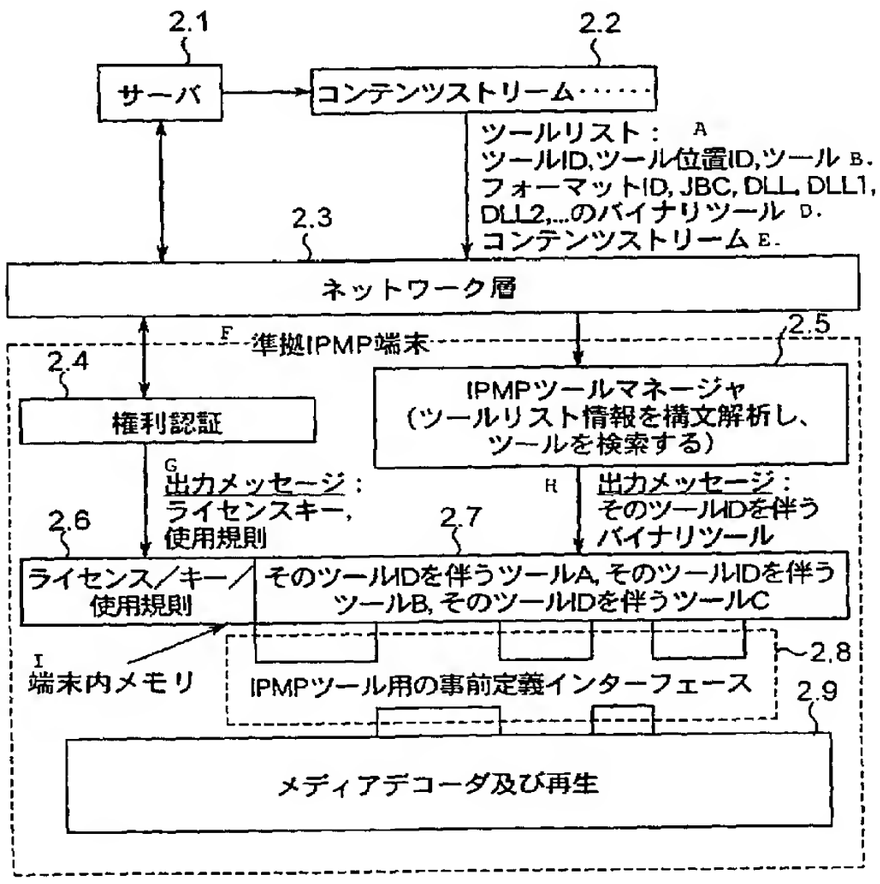
(75) 発明者/出願人 (米国についてのみ): シェン シェンメイ (SHEN,Sheng Mei) [SG/SG]; 689093 シンガポール、 ウィンダーミア・ナンバー０３−０２、チョア・チュ・カン・ストリート６４、ブロック２０ Singapore (SG). ジ ミン (JI,Ming) [CN/SG]; 389758 シンガポール、 ナンバー０２−０９、ゲイラン・イースト・アベニュー２、ブロック１０ Singapore (SG). 妹尾 孝憲 (SENOH,Takanori) [JP/JP]; 〒573-0093 大阪府 枚方市 東中振１−２４−８ Osaka (JP). 小暮 拓世 (KOGURE,Takuyo) [JP/JP]; 〒572-0020 大阪府 寝屋川市 田井西町４−１２ Osaka (JP).

(74) 代理人: 青山 葆， 外(AOYAMA,Tamotsu et al.); 〒540-0001 大阪府 大阪市中央区 城見１丁目３番７号 ＩＭＰビル 青山特許事務所 Osaka (JP).

[続葉有]

(54) Title: APPARATUS AND METHOD OF FLEXIBLE AND COMMON IPMP SYSTEM FOR PROVIDING AND PROTECTING CONTENT

(54) 発明の名称: コンテンツ提供及び保護用の柔軟及び共通ＩＰＭＰシステムの装置及び方法



2.1...SERVER
2.2...CONTENT STREAM
A...TOOL LIST
B...TOOL ID, TOOL POSITION ID, TOOL
C...FORMAT ID, JBC, DLL, DLL1
D...BINARY TOOL OF DLL2, ...
E...CONTENT STREAM
2.3...NETWORK LAYER
F...CONFORMING IPMP TERMINAL
2.4...RIGHT AUTHENTICATION

2.5...IPMP TOOL MANAGER (SYNTACTICALLY ANALYZE TOOL LIST INFORMATION AND SEARCH FOR TOOL)
G...OUTPUT MESSAGE: LICENSE KEY, USE RULE
H...OUTPUT MESSAGE: BINARY TOOL ACCOMPANIED BY TOOL ID

2.6...LICENSE/KEY/USE RULE
2.7...TOOL A ACCOMPANIED BY THE TOOL ID, TOOL B ACCOMPANIED BY THE TOOL ID, TOOL C ACCOMPANIED BY THE TOOL ID
I...IN-TERMINAL MEMORY
2.8...PRE-DEFINITION INTERFACE FOR IPMP TOOL
2.9...MEDIUM DECODER AND REPRODUCTION

(57) Abstract: An apparatus of a flexible and common IPMP (intellectual property management and protection) system gives acquiring and mutual operability to the system by fetching a complete IPMP tool list held by a content stream or downloaded from the URL position. The apparatus provides an IPMP tool manager of a conforming IPMP terminal functioning as a pre-processing module, syntactically analyzes the IPMP tool list, and acquires an IPMP tool according to the IPMP tool ID, a position identifier related to it, and the IPMP tool format ID. By pre-compiling the IPMP tool into a binary format, the IPMP tool can be transferred or downloaded to the IPMP terminal, and a different binary format is prepared by a content provider for an object on a different platform of the IPMP terminal.

[続葉有]

WO 02/100037 A1

(81) 指定国 *(国内)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) 指定国 *(広域)*: ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書
— 請求の範囲の補正の期限前の公開であり、補正書受領 の際には再公開される。

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

柔軟及び共通ＩＰＭＰシステム（知的所有権管理及び保護）の装置は、コンテンツストリームに保持された、又はＵＲＬ位置からダウンロードされた完全なＩＰＭＰツールリストを取り入れることにより柔軟性及び相互運用性を与える。前処理モジュールとして機能する準拠ＩＰＭＰ端末のＩＰＭＰツールマネージャを提供して、ＩＰＭＰツールリストを構文解析し、ＩＰＭＰツールＩＤ、それに関連する位置識別子及びＩＰＭＰツールフォーマットＩＤに基づいてＩＰＭＰツールを取得する。ＩＰＭＰツールを、バイナリフォーマットにプリコンパイルしてＩＰＭＰ端末に伝送又はダウンロードすることができ、ＩＰＭＰ端末の異なるプラットフォーム上の対象に対して異なるバイナリフォーマットをコンテンツプロバイダにより用意する。

明　細　書

コンテンツ提供及び保護用の柔軟及び共通ＩＰＭＰシステムの装置及び方法

技術分野

本発明は、コンテンツの提供及び保護に関し、特に保護コンテンツを異なるＩＰＭＰシステムにより消費する、及び同一コンテンツを異なるＩＰＭＰシステムにより保護するような用途に関する。

背景技術

コンテンツ提供は、マルチメディアデータとして益々需要が増大しており、コンテンツは、どこへでもいつでも到達可能である。ユーザは、便利さ及び柔軟性に満足しており、娯楽を容易かつ効率的に楽しむことができる。

一方、コンテンツの所有者は、顧客のニーズを満たすように努力しているが、同時に、それらのプロパティの不正使用にも苦慮している。２つの側面の間のバランスである。

前記コンテンツを保護する保護技法は、データ暗号化、透かし、暗号手法など多数ある。前記保護技法は、多くのコンテンツ提供アプリケーションで実施されている。異なるシステムが異種の機構及び保護技法を使用して保護付きのコンテンツを提供するように見える。その場合におけるすべての端末又はコンテンツ消費装置は、同一のコンテンツプロバイダにより提供されるコンテンツを実行して消費することができるだけである。前記保護技法では、それらの端末又は装置を交換して異なるコンテンツを再生することはできない。

ＭＰＥＧ標準化グループにおいて、人々は、準拠端末を含むＩＰＭＰシステムを標準化する方へ努力している。すべての端末は、たとえどのような種類のＩＰＭＰツールを使用しても、次のような同一のＩＰＭＰ標準により暗号化されて保護される保護コンテンツを再生することができる。

そのような端末は音声及び映像デコーダのようなコンテンツデコーダから成り、更に、前記端末は、前記コンテンツを復号して再生できる前に前記保護コンテン

ツから保護を解除する必要がある。従って、ＩＰＭＰツールリストを含む保護情報は、保護を解除する方法を理解するのに必要とされ、前記端末がコンテンツを利用できるのに必要とされる。

一方、ＩＰＭＰツールは予めある特定のツールに固定されない。これは、ベンダがそれらのＩＰＭＰシステムで好みのツールを選択する柔軟性をより高めることである。このような場合、より高い柔軟性とセキュリティの両方を同時に提供するのにある標準の方法及びインタフェースを定義する必要がある。

そのような端末に関する先行技術が基本的に図１に示してあり、図１は、リアルタイムでユーザ認証、ＩＰＭＰツール検索及びコンテンツ復号までの作業の流れを示す。

異なるベンダは、同一のコンテンツデコーダ、例えばＭＰＥＧ－２又はＭＰＥＧ－４を使用するけれども、前記先行技術におけるユーザ認証及びＩＰＭＰツール検索は、異なるベンダに関して全く違って実施されている。このような場合に異なるコンテンツプロバイダにより提供される異なるコンテンツを実行するのに同一の端末を製造することは非常に困難である。換言すれば、同一の保護コンテンツを異なるＩＰＭＰシステムで再生することができない。

発明の開示

（発明が解決しようとする技術的課題）

解決すべき課題は、同一のＩＰＭＰシステム構造を定義して異なるＩＰＭＰシステムが同一の保護コンテンツを消費可能にすること、及びＩＰＭＰシステム実施者に対して標準の方法を提供して安全な方法でエンコーダ、チャネル提供から端末までの全システムを構築することである。

（その解決方法）

本発明によれば、柔軟及び共通ＩＰＭＰシステム（知的所有権管理及び保護）の装置は、コンテンツストリームに保持された、又はＵＲＬ位置からダウンロードされた完全なＩＰＭＰツールリストを取り入れることにより柔軟性及び相互運用性を与える。

前処理モジュールとして機能する準拠ＩＰＭＰ端末のＩＰＭＰツールマネージャによって、ＩＰＭＰツールリストを構文解析し、ＩＰＭＰツールＩＤ、それに関連する位置識別子及びＩＰＭＰツールフォーマットＩＤに基づいてＩＰＭＰツールを取得する。

ＩＰＭＰツールを、バイナリフォーマットにプリコンパイルしてＩＰＭＰ端末に伝送又はダウンロードすることができるように、ＩＰＭＰ端末の異なるプラットフォーム上の対象に対して異なるバイナリフォーマットをコンテンツプロバイダにより用意する。

３種類の主要かつ一般的なインタフェースは、非常に有用かつ典型的な用途要件に従って、データ暗号解読、透かし埋め込み、及び透かし及びデータ暗号解読の仕方用に指定される。

本発明の一実施例では最小２層構造を提案して、ユーザ認証出力メッセージを指定し、異なるＩＰＭＰシステムに関してより高いセキュリティ及び端末互換性を与える。

端末複雑性及びＩＰＭＰツール多様性は、ＩＰＭＰツールを取得して使用する際に異なるプロファイルを指定することにより処理される。

まず第１に、ＩＰＭＰツールリストを、コンテンツストリーム内に位置するある特定のパケットとして定義し、下記の内容を示す。

・コンテンツを保護するのに使用されるＩＰＭＰツールのリスト

・ダウンロードされたＩＰＭＰツールのフォーマットＩＤ

・ＩＰＭＰツールの位置タイプ

・ＩＰＭＰツールを取得可能な位置

ＩＰＭＰツールリストフラグは、上記パケットの前にヘッダとして位置している。

ＩＰＭＰツールマネージャは、コンテンツデコーダの前に位置するあるモジュールとして設計され、コンテンツストリームに保持された、又はどこかに格納されたＩＰＭＰツールリストを構文解析して、コンテンツストリームから保護を取り外す為のＩＰＭＰツールを取得する。

汎用のインタフェースが、ダウンロードされたＩＰＭＰツールをＩＰＭＰ端末

で使用できる様にＩＰＭＰ端末用指定される。このインターフェースはある種のツールに基づいた殆どの異なるアルゴリズムを扱えるように定義される。

２層のセキュリティ構造を取り入れて、より高いセキュリティを与えると同時に、端末互換性のために任意の異なるユーザ認証方法に関する出力要件を決定する。

ＩＰＭＰツールＩＤは予め定めたテーブルで定義され、前記テーブルを事前符号化又は端末にダウンロードしておいても良い。コンテンツプロバイダ側と端末側の両方は、同一のテーブルを参照して同一のＩＰＭＰツールに同一のＩＰＭＰツールＩＤを使用する必要がある。

端末は、標準のＩＰＭＰツールと考えられているＩＰＭＰツールを事前に実装していても良いし、前記端末がダウンロード機能を有する場合、コンテンツストリームに保持されたＩＰＭＰツールリストに基づいて独自のＩＰＭＰツールをダウンロードしても良い。

暗号化キーは、前記２層セキュリティ構造に基づいて更に暗号化してＩＰＭＰ情報に挿入され、コンテンツストリームと共に端末へ伝送される。

コンテンツプロバイダ側では、メディアコンテンツは、ＭＰＥＧ－２又はＭＰＥＧ－４のような符号化技術を用いて符号化され、ＤＥＳ又はＡＥＳのようなＩＰＭＰツールを用いて暗号化される。前記コンテンツは、符号化前に透かしを埋め込まれても良い。

同時に、コンテンツＩＤは、コンテンツ著作権情報、コンテンツ作成情報などに基づいて生成される。また、ＩＰＭＰツールリストは、コンテンツを保護する際に使用されるＩＰＭＰツールに基づいて生成される。前記ＩＰＭＰツールリストは、ＩＰＭＰツールＩＤ、ＩＰＭＰツールフォーマットＩＤ、位置タイプ、ＩＰＭＰツールの位置及び予約フィールドを含む。位置識別子は、位置タイプ及び位置詳細が特定のＩＰＭＰツールＩＤに従うので、特定のＩＰＭＰツールと密接に関連がある。

ＩＰＭＰツールリストフラグは、その後に続くものがＩＰＭＰツールリストであることを示す。

任意の端末は、そのようなコンテンツを取得又は検索できるが、適切な使用ラ

イセンス及び対応する又は正しいＩＰＭＰツールなしに再生はできない。

端末側では、ＩＰＭＰツールリストをＩＰＭＰツールマネージャモジュールに渡し、ＩＰＭＰツールを取得する。

取得されたＩＰＭＰツールは、端末で使用可能なものであり、ＩＰＭＰ端末に格納されて予め定めたインタフェース用に用意がされる。

コンテンツストリームが、コンテンツデコーダを通過し始めると、ＩＰＭＰシステムは、ユーザ認証モジュールを起動して、ユーザ端末ＩＤ、コンテンツＩＤ及びその他の関連情報を与えることによりコンテンツプロバイダ又は提供エージェントにセンス要求を送信する。ライセンスは、ユーザ認証がうまく行われた後、端末に発行される。

最後に、暗号化されたキーは暗号解読され、暗号化されたコンテンツも暗号解読され、コンテンツは端末で復号及び再生可能となる。

図面の簡単な説明

図１は、先行技術のコンテンツ提供及び保護の既存ＩＰＭＰシステムを示す。

図２は、準拠ＩＰＭＰシステムの一般図を示す。

図３は、コンテンツストリームに保持されたＩＰＭＰツールリストパケットの構成を示す。

図４は、ＭＰＥＧ－４のＩＰＭＰシステムと共に作動するＩＰＭＰツールマネージャの構成を示す。

図５は、ＭＰＥＧ－２のシステムと共に作動するＩＰＭＰツールマネージャの構成を示す。

図６は、ＭＰＥＧ－４のＩＰＭＰシステム及びＩＰＭＰツールマネージャモジュールと共に作動するユーザ認証モジュールの構成を示す。

図７は、ＭＰＥＧ－２のシステム及びＩＰＭＰツールマネージャモジュールと共に作動するユーザ認証モジュールの構成を示す。

図８（ａ）は、エンコーダを有する部分的暗号化の構成を示す。

図８（ｂ）は、エンコーダを有しない部分的暗号化の構成を示す。

図８（ｃ）は、部分的暗号解読の構成を示す。

図９は、本発明の他の実施例のＩＰＭＰシステムの構成図を示す。

図１０は、本発明の実施の形態におけるＩＰＭＰシステムにおいて、プロバイダからユーザ端末に送られるメッセージの流れ図を示す。

図１１は、メッセージの具体例を示す。

図１２は、メッセージ内のＩＰＭＰ情報の一例を示す。

図１３は、利用規則管理モジュールの処理フロー図を示す。

発明を実施するための最良の形態

図１は、現在の典型的なＩＰＭＰ（知的所有権管理保護）システムを示す。

ユニット１．０のコンテンツ所有者は、ユニット１．１、１．５及び１．９の異なるコンテンツプロバイダＡ、Ｂ及びＣを通してコンテンツを提供する。異なるＩＰＭＰシステムは、３組のＩＰＭＰシステムで実施されている。

各々のプロトコルが異なるＩＰＭＰツール（例えば暗号化ツール）及び異なるユーザ認証ツールなどを使用しているので、ＩＰＭＰツールを取得して検査する方法はそれら自体のプロトコルに基づく。異なるユーザ認証方法は、ユニット１．２、１．６及び１．１０に示してあり、ＩＰＭＰツールを取得する異なる方法は、ユニット１．３、１．７及び１．１１に示してある。

従って、ユニット１．４、１．８及び１．１２に示すように、コンテンツ復号又はコンテンツ消費端末も互いに異なる。端末Ａがコンテンツプロバイダ Ｂにより提供される保護コンテンツを再生することはできないということが明らかである。

以下の内容については、本願発明者による先の出願（特願２００１－０５８２３６）において解決された。

１）ＩＰＭＰツール情報をストリームに保持して、コンテンツプロバイダ及びコンテンツディストリビュータにより何れのＩＰＭＰツールを使用するかを表示すること。

２）準拠ＩＰＭＰ端末でＩＰＭＰツール管理を用いてＩＰＭＰ情報を処理すること。

３）異なる処理能力を有するＩＰＭＰ端末に関するプロファイルを定義して、Ｉ

ＰＭＰシステムを実現すること。

しかし、先の出願では未解決の問題点が２つあり、次のとおりである。

１）端末ＯＳ及びプラットフォームに依存するダウンロードツールフォーマットの問題。

２）ＩＰＭＰ端末で使用されるべきＩＰＭＰツール用のインタフェースの問題。

本願では、更に、先の出願で提示されたＩＰＭＰシステムをより詳細かつより完全な形態で説明し、２つの問題点を詳細に扱って説明する。

図２は、ＭＰＥＧ－ｎのＩＰＭＰシステムを示す。

サーバは、モジュール２．１で示され、コンテンツプロバイダかコンテンツディストリビュータの何れかとして機能し、又は異なる用途シナリオの場合には両方の機能を果たす。

ネットワーク層は、モジュール２．３で示され、準拠ＩＰＭＰ端末とサーバとの間の通信及び前記サーバから前記端末へのコンテンツストリームの伝送を行う。

最初は、モジュール２．４の権利認証が、前記サーバと対話し始めて、権利認証モジュールの出力メッセージのような詳細な使用規則と共にコンテンツアクセス及び消費権利を得る。予め決められたフォーマットのこれらのメッセージは、後で使用されるために前記端末のメモリに格納される。出力メッセージ欄を指定する詳細については、後で説明する。

モジュール２．４でコンテンツアクセス用権利が許可されると、前記サーバは、前記ネットワーク層を介して要求されたコンテンツストリームを前記端末に送信する。

モジュール２．２では、他の専用プラットフォーム及びＯＳ用の他のフォーマットに加えてＪＢＣ（Ｊａｖａバイトコード）、ＤＬＬ（ダイナミックリンクライブラリ）などの異なるフォーマットのバイナリツールに加えて、ツールＩＤ、ツール位置ＩＤ、ツールフォーマットＩＤを含むツールリスト情報と共にコンテンツストリームを伝送する。ツールリスト情報を指定する詳細については、後で説明する。

モジュール２．５に示すＩＰＭＰツールマネージャでは、ツールリスト情報を構文解析／解釈すると同時に、ツール位置ＩＤ及びツールフォーマットＩＤ情報

に従ってＩＰＭＰツールを検索する。モジュール２．５からの出力メッセージは、ツールの内容を示す記述子用ツールＩＤを有する適切なＩＰＭＰツールである。ＩＰＭＰツール自体は、ＩＰＭＰ基準で予め決められた共通ツールフォーマットＩＤに基づいた端末プラットフォーム用に選択し検索して適合するバイナリフォーマットである。

ライセンス／キー及び使用規則は、更なる処理のためにモジュール２．６のように前記端末のメモリに格納される。対応するツールＩＤを有するバイナリＩＰＭＰツールは、モジュール２．７のように前記端末のメモリに格納される。前記ツールの各々は、一般的な標準化インタフェースに従って構築され、プラットフォームに適合させる為にコンパイラを用いてプリコンパイルされる。例えば、データ暗号化及び暗号解読のツールは、１つの汎用指定インタフェースに基づいて構築可能である。たとえば、Ｊａｖａ仮想マシンで全プラットフォーム／端末用のＪａｖａバイトコード（ＪＢＣ）にプリコンパイル可能であり、またＷｉｎｄｏｗｓによるプラットフォーム／端末用のダイナミックリンクライブラリ（ＤＬＬ）にプリコンパイル可能である。

バイナリ形式のツールは、ｚｉｐ形式などの圧縮形式で伝送可能である。前記ツールは、不正変更防止ソフトウェアを用いることにより不正変更可能であり、又は、バイナリコードが破られる又はハッキングされるのを防ぐ署名技法を用いて署名可能である。

モジュール２．８は、ＩＰＭＰツールプロバイダ及び端末実施者が予め定められ従うことが必要なＩＰＭＰツール用のインタフェースを示す。

ベース層は、モジュール２．９に示すコンテンツデコーダ及びプレゼンタである。この層は、前記ベース層の他の構成要素に位置して前記構成要素とともにスムーズに動作するバイナリ形式でＩＰＭＰツール用のフックインタフェースを用いて構築される。

汎用インタフェースは、３種類のＩＰＭＰツール（暗号解読用インタフェース、透かし埋め込み用インタフェース、透かし技能と暗号解読用インタフェース）について後で明記する。権利認証用インタフェースは、用途に大きく左右されるので予め定義することができず、そのため、ここで定義及び固定されるのではなく

パラメトリックツールにより処理される。

詳細な説明をここで４つの部分に分けて、説明する。

１．　ＩＰＭＰツールリスト及びＩＰＭＰツールマネージャ

１．１　ＩＰＭＰツールリスト及びＩＰＭＰツールマネージャの定義

ＩＰＭＰの概要において、ＩＰＭＰ情報は、所与のＩＰＭＰツールが所与の保護コンテンツを要求して正しく処理する情報と定義されている。

ＩＰＭＰツールは、予め決められた方法で認証、暗号化、透かしなどのＩＰＭＰ機能を実行するモジュールであると定義されている。

この発明において、ＩＰＭＰツールリストの定義を導入する。

ＩＰＭＰツールリストは、ＩＰＭＰツールマネージャがＩＰＭＰツールを識別して前記ＩＰＭＰツールを検索する必要がある情報を含む。それは、ＩＰＭＰツールの一意的識別、ＩＰＭＰツールの位置識別子、及びＩＰＭＰツールＩＤとコンテンツＩＤとの間の関係定義を含む。

また、ＩＰＭＰツールマネージャを次のように定義する。

ＩＰＭＰツールマネージャは、その唯一の役割がＩＰＭＰツールリストを処理してコンテンツストリーム全体を消費するのに必要なＩＰＭＰツールを検索するエンティティである。

１．２　ＩＰＭＰツールリスト

このＩＰＭＰツールリストパケットの詳細構造は、次のような図３に最もよく示されている。

前記ＩＰＭＰツールリストパケットは、保護コンテンツを消費するのに必要な全ＩＰＭＰツールの情報を含む。前記コンテンツが２種類以上のコンテンツを含む場合、例えば、前記コンテンツの第１の部分はコンテンツプロバイダＡからであり、第２の部分はコンテンツプロバイダＢから来ている場合、個々のＩＰＭＰツールに関連する情報は、それぞれ関連するコンテンツＩＤごとに分類される。

次に、各コンテンツＩＤ用のＩＰＭＰツールリストは、個々のＩＰＭＰツール情報から成れば良く、これらの個々のＩＰＭＰツール情報の順序は重要でない。

各ＩＰＭＰツール情報は、３つの主要な部分、即ちＩＰＭＰツールＩＤ、ＩＰＭＰツール位置識別子及びＩＰＭＰフォーマットＩＤから成る。

前記ＩＰＭＰツールＩＤは、所定の方法でツールを識別し、少なくとも２つの部分、ツールタイプＩＤ及びツールサブＩＤを有する。

ツールタイプＩＤは、この特定のＩＰＭＰツールが（ツール機能の点から）何れのカテゴリ、例えば暗号解読、透かし抽出、透かし検出、権利抽出などに属するかを指定する。下記の表は、ＩＰＭＰツールの１６カテゴリを扱うことができる４ビットとしてツールタイプＩＤの長さを仮に設定する。

更に、ツールサブＩＤはある特定のＩＰＭＰツールを識別し、前記サブＩＤは、下記の表のように、１ツールタイプ間の４０９６の異なるツールを識別することができる長さ１２ビットとして仮に設定される。

【表１】

ＩＰＭＰツールＩＤリスト

ツール機能	IPMPツール ID	IPMPツール名前	注
暗号解読ツール	... 0001 000000000000 ...	DESDecrypt	１２ビットにより４０９６の異なるツールが可能になる
	... 0001 000000000001 ...	AESDecrypt	
	... 0001 000000000010 ...	SC2000Decrypt	
	... 0001 000000000011 ...	CamelliaDecrypt	
	... 0001 000000000100 ...	Xxxx	
	... 0001 000000000101 ...	Xxxx	
	... 0001 000000000110 ...	Xxxx	
	... 0001 000000000111 ...	Xxxx	
	... 0001 000000001000 ...	Xxxx	
	... 0001 00000000xxxx ...	Xxxx	
	... 0001 00000000xxxx ...	Xxxx	
	... 0001 100000000000 ...	予約	今後／独占ツールに予約
	... 0001 100000000001 ...	予約	
透かし埋め込みツール	... 0010 000000000000 ...	透かしツール１	１２ビットにより４０９６の異なるツールが可能になる
	... 0010 000000000001 ...	透かしツール２	
	... 0010 000000000010 ...	透かしツール３	
	... 0010 000000000011 ...	Xxxx	
	... 0010 000000000100 ...	Xxxx	
	... 0010 00000000xxxx ...		
			今後／独占ツールに予約
		予約	
		予約	

注：上記の最初の４ビットはツールタイプＩＤである

この表は端末に事前ロードされるべきであり、又は、端末は上記に示す標準化ツールＩＤ表に基づいて構築される。

位置識別子は転送機構を暗示し、１つのＩＰＭＰツールに関して２つ以上の位置識別子が可能である。ＩＰＭＰツールマネージャは、前記識別子の各々を用いて前記ツールを検索しようと試みる。ＩＰＭＰツールＡの第１の位置識別子が成功した場合、次の位置識別子がスキップされ、さもなければ、第２の位置識別子に続く。

例えば、位置識別子は下記の様に記述される。

１．ローカル：端末システムの内部又は周辺装置

２．外部：指定された端末システムの外部（ｈｔｔｐ：，ｆｔｐ：）

ＩＰＭＰツール識別子は、２つの部分（位置タイプ及び位置詳細）から成る。位置タイプは、次のうちの１つでなければならない。位置タイプと位置詳細との間の対応は、表２に示されている。

【表２】

可能な位置タイプとそれらの詳細

位置タイプＩＤ	位置タイプ	位置詳細
0000	“ローカル”	N/A
0001	“周辺装置”	N/A
0010	“遠隔－ダウンロード可能”	Website(http, ftp ...)
0011	“遠隔－ダウンロード不可能”	Java serveletなどの遠隔位置
0100	“コンテンツストリーム内部”	この部分はＩＰＭＰツール自体を含むべきである
...	...	...
1***	予約	予約

ツールフォーマットＩＤは、ＩＰＭＰツールＩＤ及びツール位置ＩＤと共に伝送され、通知するのに８ビットを用いており表３に明記されている。

提供されたＩＰＭＰツールが何れのバイナリフォーマットであるかをＩＰＭＰ端末は、ＤＬＬ、ＪＢＣ、又はその他などのツールフォーマットＩＤから知り、前記ＩＰＭＰ端末は、そのＯＳと合致する適切なフォーマットで前記ツールをダ

ウンロード又は検索できる。

【表３】

ダウンロードされたＩＰＭＰツールのフォーマットＩＤ

８ビット	ダウンロードされたフォーマット	対象プラットフォーム	コンパイラ	ＩＰＭＰ端末
00000000	JBC (Javaバイトコード)	JVMインタプリタ埋め込みマシン	Javaコンパイラ	殆どの携帯電話及びSTBs
00000001	DLL1	Windowsマシン	Microsoft C コンパイラ	Windows上で実行中の全PC
00000010	DLL2	Unix マシン	gcc及び他のコンパイラ	全Unix, Linux OS
00000011				
予約	DLL-AM33	パナソニックのチップ	AM33 コンパイラ	チップ依存の製造に予約、及び特定のコンパイラを必要とする
予約				
予約				
予約				

ダウンロードされるＩＰＭＰツールのツールフォーマットＩＤを定義して端末相互運用性を達成する目的は、次の通りである。

１　最近、殆どの携帯電話及びＤＴＶ　ＳＴＢは、Ｊａｖａ仮想マシン（ＪＶＭ）で構築されており、ストリーム内の保持又はＵＲＬからのダウンロードを介してＩＰＭＰツールをＪａｖａバイトコードにコンパイルして端末にダウンロードすることができる。

２　ＤＬＬは、ＰＣ又はＵｎｉｘで使用される非常に普及しているフォーマットである。異なるビット数のフラグを使用して、ユーザの端末が何れのＤＬＬフォーマットをダウンロードする必要があるかを通知する。

３　ＪＶＭも標準Ｃ／Ｃ＋＋コンパイラも有しない他の端末に関して、例えば、あるＤＴＶ　ＳＴＢに、ＩＰＭＰツールを、それらのコンパイラを用いてプリコンパイルしブロードキャストストリーム又は裏チャネルを介してダウンロードすることができる。これは、放送業者又は製造業者がそれらのソフトウェアを更新したい時に現在ＤＴＶ　ＳＴＢが行っていることである。

この場合、前記表の同じ予約ビットフラグを、放送業者と製造業者の両方により選択及び参照して、前記業者がＩＰＭＰツールの何れのフォーマットを検索して使用することができるかをＤＴＶ　ＳＴＢに通知する。

ＩＰＭＰツールリスト用構文は、次の通り定義される。

【数１】

```
class IPMP_Tool_List
{
        bit(128) IPMP_Tool_ID;
        //whether this IPMP Tool is a parametric tool or normal tool is
implicitly
        // indicated by the IPMP_Tool_ID.
        if (parametricRepresentation)
        {
                //... detailed syntax of parametric representation.
        }
        else
        {
        bit(1)  hasAlternativeToolLocation;
        while (hasAlternativeToolLocation)
        {
                bit(1)  hasAlternativeToolLocation;
                bit(7)  Tool_Location_ID;
                if (Tool_Location_ID == 0b0000000) //tool carried in
bitstream.
```

```
{
}
else if (Tool_Location_ID == 0b0000001) //remote method
call
{
    bit(8) Remote_Call_Mechanism; //CORBA, DCOM, RMI,
    //SOAP ...
      bit(1) Client_In_Bitstream;
}
else if (Tool_Location_ID == 0b0000010 ||
Tool_Location_ID=0b0000011)
    // Remote Downloadable, http protocol or ftp
  protocol
{
    bit(8)  Tool_Format_ID;
    unsigned int(16) serverAddressLen;
    bit(8) serverAddress[serverLen];
    unsigned int(16) fullPathLen;
    bit(8) fullPath[fullPathLen];
    bit(1) isCompressed;
    if (isCompressed)
    {
        bit(7) compressionMethod;
    }
}
else if (Tool_Location_ID == 0b0000100 .. 0b1000000)
//ISO reserved
    {
    }
```

```
                else // user defined.
                {
                }
            }
        }
    }
```

意味

ＩＰＭＰ＿Ｔｏｏｌ＿ＩＤは、ユニバーサルレベルでツールを一意に識別する。最初の１６ビットは特定のＩＰＭＰツールのタイプカテゴリを識別するのに対して、次の１１２ビットは前記ＩＰＭＰツールを詳細に識別する。下記の表に、前記ＩＰＭＰ＿Ｔｏｏｌ＿ＩＤを説明する。登録当局が、そのような表を保守する責任を持つ。

幾つかの通常用いられるＩＰＭＰツールを標準化する必要があり、それらの基本的なＩＰＭＰツールを含むテーブルを定義する必要があり、このテーブルをあらゆるＩＰＭＰ端末に事前ロードするべきである。下記の表はこの考えを説明する。標準化されるべき基本ツールの内容に関して、それはＩＰＭＰ委員会で更に論議する事項である。

Ｔｏｏｌ＿Ｌｏｃａｔｉｏｎ＿ＩＤは、転送機構を暗示し、ツールがコンテンツストリームに保持されるか、遠隔位置からダウンロードする必要があるか、又はＩＰＭＰツールが遠隔位置で実行可能であるか否かを示す。

１つのＩＰＭＰツールに関して２つ以上の位置識別子が可能である。ｈａｓＡｌｔｅｒｎａｔｉｖｅＴｏｏｌＬｏｃａｔｉｏｎは、ＩＰＭＰツールがべつの検索先を有するか否かを示す。ＩＰＭＰツールマネージャは、前記識別子の各々を用いて前記ツールを検索しようと試みる。ＩＰＭＰツールＡの第１の位置識別子が成功した場合、次の位置識別子がスキップされ、さもなければ、第２の位置識別子が調べられる。

【表４】

ＩＰＭＰツール位置識別子（ＩＰＭＰ　Ｔｏｏｌ＿Ｌｏｃａｔｉｏｎ＿ＩＤ）

Tool_Location_ID	位置タイプ
000 0000	コンテンツストリームの内部に保持されたツール
000 0001	遠隔位置で実行されるツール
000 0010	httpプロトコルによるダウンロード
000 0011	ftpプロトコルによるダウンロード
000 0100 -- 100 0000	ISO予約
100 0001 -- 111 1111	予約

Ｔｏｏｌ＿Ｌｏｃａｔｉｏｎ＿ＩＤが０ｂ００００００００である場合、それは、ＩＰＭＰツールがコンテンツストリームに保持されていることを意味する。Ｍｐｅｇ４データにおいて、本発明では、ＩＯＤと関連のある提案されたＩＰＭＰツールＥＳ内にバイナリＩＰＭＰツールを入れる。その詳細は、後で説明する。

Ｔｏｏｌ＿Ｌｏｃａｔｉｏｎ＿ＩＤが０ｂ００００００００１である場合、それは、このＩＰＭＰツールが遠隔側で実行されるものであることを意味し、ＩＰＭＰ端末は、ＲＰＣ（遠隔手続き呼び出し）を介してこのＩＰＭＰツールを呼び出す。８ビット遠隔呼び出し方法は、このＩＰＭＰツールが何れのＲＰＣ機構、例えばＣＯＲＢＡ、ＲＭＩ、ＸＭＬ－ＲＰＣ、ＤＣＯＭに対応しているかを示す。このＲｅｍｏｔｅ＿Ｃａｌｌ＿Ｍｅｃｈａｎｉｓｍに関する詳細は、下記の表で定義される。ＩＰＭＰツールマネージャは、前記端末が前記ＲＰＣ機構に対応しているか否かをチェックする。

【表５】

ＩＰＭＰ　Ｒｅｍｏｔｅ＿Ｃａｌｌ＿Ｍｅｃｈａｎｉｓｍ

Remote_Call_Mechanism	RPC機構
0000 0000	DCOM
0000 0001	RMI
0000 0010	CORBA
0000 0011	XML-RPC
0000 0100	SOAP
… …	… …
0000 1000 -- 1000 0000	ISO予約
1000 0001 -- 1111 1111	予約

前記ＩＰＭＰツールが遠隔で実行されるものである場合、ＩＰＭＰ端末は、遠隔ＩＰＭＰツールとインタフェースをとって通信するクライアントのような軽量コードを必要とする。例えば、前記遠隔ＩＰＭＰツールがＣＯＲＢＡを介して呼び出されることができるだけである場合、前記ＩＰＭＰ端末は、ＩＩＯＰ（インターネットＯＲＢ間プロトコル）を介して前記遠隔ＩＰＭＰツールに適切にパラメータをひとまとめに伝達する方法を知っているスタブを必要とする。本発明では、この軽量バイナリコードをＩＰＭＰツールクライアントとして呼び出す。ＩＰＭＰツールクライアントは軽量であると考えられているので、それは可能であり、コンテンツストリーム内に保持される。このＩＰＭＰツールクライアントをコンテンツストリーム内に保持する方法は、後で説明する。

遠隔で実行されるＩＰＭＰツールと通信するＩＰＭＰツールクライアントを有するだけでは、ＩＰＭＰ端末がこの遠隔ＩＰＭＰツールを利用することを可能とするのに十分でない。ＩＰＭＰ端末は、前記ＩＰＭＰツールクライアントを初期設定してそれに話しかける方法を必要とする。これを処理する方法は、この提案の範囲外である。この面において、ＩＰＭＰツールクライアントは他の通常のＩＰＭＰツールと同じように見える。従って、前記ＩＰＭＰツールを丁度他のＩＰＭＰツールのように初期設定して呼び出すべきであり、例えば、ＩＰＭＰツールクライアントとＩＰＭＰ端末との間のインタフェース定義は、このＩＰＭＰツールクライアントが動作することになっているＯＤ又はＥＳＤ間のＩＰＭＰ記述子に保持されても良い。

Ｔｏｏｌ＿Ｌｏｃａｔｉｏｎ＿ＩＤが０ｂ０００００１０である場合、それは、ＩＰＭＰツールマネージャがｈｔｔｐプロトコルによって特定のＩＰＭＰツールをダウンロードすべきであることを意味する。０ｂ０００００１１は、ｆｔｐプロトコルを使用すべきであることを意味する。ＳｅｒｖｅｒＡｄｄｒｅｓｓ（例えば、ｗｗｗ．ｐａｎａｓｏｎｉｃ．ｃｏｍ）及びｆｕｌｌｐａｔｈ（例えば、／ｉｐｍｐｔｏｏｌｓ／ｅｎｃｒｙｐｔｉｏｎ／ｔｏｏｌ１．ｚｉｐ）は、この特定のＩＰＭＰツールを検索する場所をはっきりと定義する。ＩＰＭＰツールマネージャがｈｔｔｐ又はｆｔｐプロトコルを実施して必要なＩＰＭＰツールを検索する方法は、本発明の応用課題である。特定のＩＰＭＰツールを検索するのに使用可能な複数種のプロトコル（ｈｔｔｐｓ、ｓｓｌ）がある場合もある。ＩＳＯ予約ビット範囲０００００１００－－１０００００００は、複数種のプロトコルを保持する様に設計されている。

ＩＰＭＰツールプロバイダがそれ自身の独占プロトコルを使用したい場合には、ビット範囲１０００００１－１１１１１１１を使用すれば良い。

ＩｓＣｏｍｐｒｅｓｓｅｄビットは、指定ツールが圧縮されているか否かのフラグを立てる。圧縮されている場合、ＩＰＭＰツールマネージャは、ｃｏｍｐｒｅｓｓｉｏｎＭｅｔｈｏｄ欄に明示の圧縮方法に従って前記ツールを伸張する必要がある。ＰＣ用圧縮方法は多数あり、とりわけＰＫＺｉｐ、ＬＨＡｒｃ、ＡＲＪ、及びＺＯＯがある。マッキントッシュでは、ＳｔｕｆｆＩｔ、ＣｏｍｐａｃｔＰｒｏ及びその他がある。複数の圧縮方法をＩＰＭＰで使用できる様にすることもでき、又は１つの圧縮方法をデフォルトとして指定することもできる。

ＩＰＭＰ＿ＴｏｏｌＥＳ

Ｍｐｅｇ４システムのデータにおいて、本発明では、基本ストリーム間に（前記で提案したＩＰＭＰツールクライアントを含む）バイナリＩＰＭＰツールを保持する。その目的を果たすために、本発明では、基本ストリームに対応付けられたデコーダ構成記述子に新しいストリームタイプを定義する。

ストリームタイプ“ＩＰＭＰＴｏｏｌＳｔｒｅａｍ”を以下の様に、提案する。０ｘ０Ａ－０ｘ１ＦがＩＳＯ使用のために予約されているので、このストリームタイプに割当てられる値を０ｘ０Ａと設定する。従って、Ｍｐｅｇ４システム仕

様の現バージョンで定義されたストリームタイプ表を、下記のように変更する。

【表６】

ＩＰＭＰ　Ｒｅｍｏｔｅ＿Ｃａｌｌ＿Ｍｅｃｈａｎｉｓｍ

ストリームタイプ値	ストリームタイプ記述
0x00	禁止
0x01	ObjectDescriptorStream (ISO/IEC 14496-1 参照)
0x02	ClockReferenceStream (ISO/IEC 14496-1 参照)
0x03	SceneDescriptionStream (ISO/IEC 14496-1 参照)
0x04	VisualStream
0x05	AudioStream
0x06	MPEG7Stream
0x07	IPMPStream (ISO/IEC 14496-1 参照)
0x08	ObjectContentInfoStream (ISO/IEC 14496-1 参照)
0x09	MPEGJStream
0x0A	IPMPToolStream
0x0B - 0x1F	ISO 使用に予約
0x20 - 0x3F	ユーザ専用

前記ＩＰＭＰＴｏｏｌＳｔｒｅａｍを復号するデコーダは、ＩＰＭＰツールマネージャである。０ｘ０Ａのストリームタイプを参照する際に、ＩＰＭＰ端末は、構文解析するＩＰＭＰツールマネージャに前記基本ストリームを渡す。ＩＰＭＰＴｏｏｌＳｔｒｅａｍは、初期オブジェクト・デスクリプタＯＤに通常置かれている。

ＩＰＭＰ＿Ｔｏｏｌ ＥＳの構文

【数２】

```
class IPMP_ToolES
{
        IPMP_Tool ipmp_tools[0 .. 255];
}

class IPMP_Tool
{
        bit(128) IPMP_Tool_ID;
```

```
bit(8)   Tool_Format_ID;
bit(1) isCompressed;
if (isCompressed)
{
        bit(7) compressionMethod;
}

bit(1) isSigned;
  if (isSigned)
  {
        bit(8) signature_Algorithm[];
        bit(8) signature_Parameters[];
    bit(1) IPMP_Tool_List_Signature[];
  }
    bit(16) Tool_Size;
    bit(Tool_Size) Tool_Body;
}
```

ＩＰＭＰ＿Ｔｏｏｌ ＥＳの意味

ＩＰＭＰ＿Ｔｏｏｌ＿ＩＤ、Ｔｏｏｌ＿Ｆｏｒｍａｔ＿ＩＤは、前記で定義されている内容と同じ意味を有する。

前記基本ストリームに保持されたＩＰＭＰ＿Ｔｏｏｌは、ＩＰＭＰ＿Ｔｏｏｌの保全性を保証するのにある特定の署名アルゴリズムを用いて署名可能である。

前記署名の確認後、ＩＰＭＰツールマネージャは、Ｔｏｏｌ＿Ｓｉｚｅにより指定されたサイズのＴｏｏｌ＿Ｂｏｄｙをハードディスク又は物理メモリに適切に格納する。前記端末又はメッセージルータは、そのことを認識している。

前記ＩＰＭＰＴｏｏｌＳｔｒｅａｍに保持可能なＩＰＭＰツールは、提案したＩＰＭＰツールクライアントを含む。基本ストリームからの検索及びＩＰＭＰ端末による初期設定の後、ＩＰＭＰツールクライアントは、遠隔ＩＰＭＰツールと対話する。しかし、前記端末にとって、前記ＩＰＭＰツールクライアントは、一

意のＩＰＭＰ＿Ｔｏｏｌ＿ＩＤを有する通常のＩＰＭＰツールとあまり違わない。

１．３　ＩＰＭＰツールマネージャ

ＩＰＭＰツールマネージャは、システムのデマルチプレクサの前又は後に位置することができる。その機能性は、コンテンツストリーム内にあるＩＰＭＰツールリストを構文解析することである。

図４に示す線図は、ＩＰＭＰツールマネージャがＭｐｅｇ４－ＩＰＭＰシステムに組み込まれた例を示す。

ＩＰＭＰツールマネージャは、次の４つのステップを実行する。

・ステップ１：入力ＩＰＭＰデータをＩＰＭＰツールリストを求めて構文解析する。前記リストがない場合、ステップ４に進み、他の場合、正規の構文に従って前記ＩＰＭＰツールリスト間のＩＰＭＰツール情報を構文解析する。

・ステップ２：すべての要求ＩＰＭＰツールが端末に入手できる場合、ステップ４に進む。

・ステップ３：ＩＰＭＰツール情報で指定された必要なＩＰＭＰツールを検索し、検索が成功しない場合、中止し、他の場合、ステップ４に進む。

・ステップ４：全ＩＰＭＰツールをうまく取得した後、アクセス許可がある場合、利用可能なコンテンツは、データバッファに流れ始めることが可能となる。

コンテンツストリームを受信する際に、ＩＰＭＰツールマネージャは、あらゆるコンテンツストリームに関する一意のヘッダであるＩＰＭＰツールリストパケットフラグを捜すことにより前記コンテンツストリームをまず調べる。ＩＰＭＰツール情報パケットの前記フラグが見つからない場合、ステップ４にジャンプする。

第３のステップにおいて、ＩＰＭＰツールマネージャは、位置識別子タイプＩＤ及び位置識別子詳細を調べることにより各ＩＰＭＰツールを検索しようと試みる。１つのＩＰＭＰツールに対応付けられた２つ以上の位置識別子がある場合、前記ＩＰＭＰツールマネージャは、まず位置識別子１を用いて前記ＩＰＭＰツールを検索しようと試み、それが失敗した場合、次に位置識別子２を用いて検索しようと試みる。

位置識別子タイプが「ローカル」の場合、ＩＰＭＰツールマネージャは、指定

されたＩＰＭＰツール名前又はＩＰＭＰツールＩＤに従って端末自身の中を探索する。

位置識別子タイプが「周辺装置」の場合、ＩＰＭＰツールマネージャは、指定されたＩＰＭＰツール名前又はＩＰＭＰツールＩＤに従ってすべての周辺装置を探索する。

位置識別子タイプが「遠隔ーダウンロード可能」の場合、ＩＰＭＰツールマネージャは、指定された遠隔アドレスに接続し、必要ならば、相互に受入れ可能な通信チャネルをＩＰＭＰツールマネージャとツールプロバイダとの間にセットアップする。

位置識別子タイプが「遠隔ーダウンロード不可能」の場合、ＩＰＭＰツールマネージャは、前記遠隔アドレスをＩＰＭＰシステムに渡すだけである。

位置識別子タイプが「コンテンツストリーム内部」の場合、ＩＰＭＰツールマネージャは、ツールフォーマットＩＤをチェックすることにより端末に適合するバイナリフォーマットで前記ツールをロードし、ツール記述子として格納されたツールエンティティにＩＰＭＰツールＩＤを割当てる。

デマルチプレクサインターフェス３０４の後に、音声デコーダバッファ３０６、映像デコーダバッファ３０７、ＩＰＭＰツールデコーダバッファ３０１、オブジェクトディスクリプタデコーダバッファ３０８、バイナリデータフォアシーン（binary data for scene）（ＢＩＦＳ）デコーダバッファ３０９、ＩＰＭＰデコーダバッファ３１０が含まれる。バイナリデータフォアシーンは、セグメント化されたシーンの配置場所を示すデータが含まれる。３０６，３０７，３０９の出力である、音声信号、映像信号、ＢＩＦＳ信号はまだ暗号化されたままの状態である。メモリ３０２にはツールA（一つ、又は複数）が各端末に予めインストールされている。

音声デコーダバッファ３０６は制御ポイント３３１を介して音声復号３１１に接続され、映像デコーダバッファ３０７は制御ポイント３３２を介して映像復号３１２に接続され、オブジェクトディスクリプタデコーダバッファ３０８は、そのままオブジェクトディスクリプタ復号３１３に接続され、バイナリデータフォアシーン（binary data for scene）（ＢＩＦＳ）デコーダバッファ３０９は制御

ポイント３３３を介してＢＩＳＦ復号３１４に接続される。また、ＩＰＭＰデコーダバッファ３１０は、ＩＰＭＰメッセージルータ３２４のＩＰＭＰエレメンタリーストリーム３２５に接続される。ＩＰＭＰエレメンタリーストリーム３２５には暗号化されたスクランブルキーが保持されている。

図において、黒丸で示された制御ポイント３３１～３３９は、ＩＰＭＰ制御ポイントであり、制御ポイントを通過するデータは、ＩＰＭＰシステム３２４にあるツールを利用して、必要な処理（デスクランブル、透かし検出、コピーガード等）が加えられる。

この実施の形態では、制御ポイント３３１，３３２，３３３ではデスクランブルが行なわれる。デスクランブルに必要なツール（ソフト）は、ＩＰＭＰメッセージルータ３２４、端末ーツールメッセージインターフェース３２１を介してＩＰＭＰツール１、2、又は3から取得する。

音声復号３１１は、制御ポイント３３４を介して音声コンポジタバッファ３１５に接続され、映像復号３１２は、制御ポイント３３５を介して映像コンポジタバッファ３１６に接続され、ＢＩＦＳ復号３１４は、制御ポイント３３６を介して復号ＢＩＦＳ３１７に接続される。

制御ポイント３３４，３３５，３３６では透かし検出が行なわれる。透かし検出に必要なツール（ソフト）は、ＩＰＭＰメッセージルータ３２４、端末ーツールメッセージインターフェース３２１を介してＩＰＭＰツール１、2、又は3から取得する。例えば、ＩＰＭＰツール２は、デスクランブルに必要なツールが保持されており、ＩＰＭＰツール３は、透かし検出に必要なツールが保持されている。

音声コンポジタバッファ３１５は、制御ポイント３３７を介して合成器３１８に接続され、映像コンポジタバッファ３１６は、制御ポイント３３８を介して合成器３１８に接続され、復号ＢＩＦＳ３１７は、制御ポイント３３９とＢＩＦＳツリー３１９を介して合成器３１８に接続される。合成器３１８は更に出力であるレンダリング３２０に接続される。

制御ポイント３３７，３３８，３３９では別の透かし検出や、コピーガード処理が行なわれる。透かし検出やコピーガード処理に必要なツール（ソフト）は、

ＩＰＭＰメッセージルータ３２４、端末ーツールメッセージインターフェース３２１を介してＩＰＭＰツール１、2、又は３から取得する。

ＩＰＭＰツールマネージャ３００は、ＩＰＭＰツールリストを解析する解析部３５０と、ＩＰＭＰツールを検索する検索部３５１がある。オブジェクトディスクリプタデコーダバッファ３０８は、そのままオブジェクトディスクリプタ復号３１３に接続され、コンテンツストリームに含まれるオブジェクトディスクリプタを復号する。復号されたオブジェクトディスクリプタは、ＩＰＭＰツールマネージャ３００に送られ、必要とされるツールが存在する位置について特定がなされ、そのツールを取得するためのデータがＩＰＭＰツールマネージャ３００からツールメッセージインターフェース３２１に送られる。ツールメッセージインターフェース３２１は、特定されたツールがメモリ３０２にあればそのツールをＩＰＭＰツール２または３に移動し、必要な処理を行なう。特定されたツールがメモリ３０２にない場合は、インターネットなどの伝送路を介し、リモートツール３６０にアクセスし、必要なツールをＩＰＭＰツール１にダウンロードする。また、必要なツールが遠隔ＩＰＭＰツールＢ３６２にしかなく、ダウンロードが出来ない場合は、暗号化されたデータをそのまま、ＩＰＭＰツールＢのローカルクライアント３６４を介して遠隔ＩＰＭＰツールＢ３６２に送り、遠隔ＩＰＭＰツールＢ３６２で解読したデータを送り返す様に動作する。

ＩＰＭＰツールマネージャ及びＩＰＭＰツールリストを含むこのアーキテクチャは、任意のＭＰＥＧ－ｎシステムに適用でき、図５は、ＩＰＭＰツールマネージャがＭＰＥＧ２－ＩＰＭＰシステムに組み込まれる場合を示す。ここに示す例では、オブジェクトが含まれない。PESで示される黒丸で示す制御ポイントにおいてデスクランブルや、透かし情報の解読が行なわれる。

コンテンツの同一部分に対しては、ＭＰＥＧ－ｎのＩＰＭＰシステムに関する一般的な構文は、次のような流れで定義可能である。

【数３】

```
Class    UserAuthentication( )
{
        Class       ReceivingContentStream( )
```

```
{
        Class       DemuxContent( )
        {
            Class   IPMPToolsManagement( )
            {
                Class ParseIPMPToolsInformation( ); //IPMP Tool
                      Management module, see 2.3 for details;
                Class RetriveIPMPTools( );              //IPMP
                      Tool Management module, see 2.3 for
                      details;
                  {
                Class     ContentConsumptionStart( );
                }
                }
            }
        }
}
```

２．　ユーザ権利認証に指定されるべき出力メッセージ

ユーザ権利認証（ＲＡ）方法を標準化することは勧められていないけれども、認証結果又はＲＡ用出力メッセージは、基準を定めたり、又は予め定める必要がある。このメッセージは、保護コンテンツの許可使用のためにＭＰＥＧ－ｎのＩＰＭＰシステムを通過する必要がある。

我々は、認証出力メッセージを標準規格として設定すべきであることを提案し、その標準は、下記のように少なくとも３つのフィールドから成るべきである。

【表７】

有効性 (真／偽)	ライセンス	利用ルール	空

ユーザ権利認証（ＲＡ）の機能に関する構文は、次の通りリストされる。

【数４】

```
Class   RightAuthenticationMessages( )
{
        bit(1) Valid;
        if(valid)
        {
                Class   RetrieveLicence( );
                Bit(16) Licence;
                Class   UsageRule( );
                Bit(length)     UsageRule;
        }
}
```

妥当性は、ユーザ（端末）が正当であるか否かを示し、その結果は単なる真又は偽の表示でもよい。使用規則は、コンテンツにアクセスするユーザ権利の詳細を含むべきである（例えば、１回又は複数回のプレー）。ライセンスは、以下に説明する。

ＩＰＭＰデータに示すように（例えば、Ｍｐｅｇ４－ＩＰＭＰのＩＰＭＰ－ＥＳ）、コンテンツにスクランブルがかけられ、そのスクランブルキーをコンテンツストリーム内に伝送することが知られている。例えば、ＩＰＭＰ－ＥＳには暗号化されたスクランブルキーが入っている。より高いセキュリティを確保するために、前記スクランブルキーは、２層のセキュリティを達成するよう更に暗号化可能である。スクランブルがかけられているコンテンツ用のスクランブルキーを暗号解読するのに使用される第２層のキーは、「ライセンス」と呼ばれる。「ライセンス」は、保護コンテンツを消費する最小要件である。ライセンスは、非基準ユーザ認証処理の間に安全なチャネルを介してライセンスサーバから検索されるべきである。

上記認証出力メッセージは、たとえＩＰＭＰ端末がどんな種類のユーザ認証方法を使用しても、ユーザ認証中に提供されて出されるべきである。

ここで使用規則は、消費タイプ及び規則用のバイナリフォーマットに関する表

４で更に定義可能である。代わりに、前記使用規則を、バイナリフォーマットではなくＸＭＬフォーマットで定義して対話することもできる。

【表８】

バイナリフォーマットで定義された消費タイプ及び規則

消費タイプ	８ ビット	消費規則タイプ ４ ビット+変数	注
アクセス	00000000		アクセスコンテンツ
プレー（ストリーミング）	00000001		ストリーミング再生
格納及びプレー	00000010		格納及び再生
		0001 + プレーカウント	
		0010 + プレー時間	
		0011 + プレー期間	
		0100 +コピーカウント	
		0101 +移動カウント	
		予約	
シーングラフ編集	00000011		
時間ライン編集	00000100		
テキスト又はその他の追加			
	予約		

図６に示す線図は、ＭＰＥＧ－４のＩＰＭＰシステムと共に作動するユーザ認証モジュールを示し、ユーザ認証の実行後にコンテンツエージェントを要求してライセンスをユーザに発行する。ユーザＩＤ情報は、ＩＰＭＰシステム内に含まれている。このユーザＩＤ情報が標準では定義しないユーザ認証においてユーザＩＤの照合が行なわれる。この照合には例えば乱数が用いられる。照合が成立すれば、正しいユーザとしてサーバに対しユーザ登録を行なう。

図７の線図に示すように、２重セキュリティ構造は、ＭＰＥＧ－ｎのＩＰＭＰに関して実現可能である。サーバから送られてきたライセンスキーは、ＩＰＭＰツール保持部に送られる。また、コンテンツストリームに含まれる暗号化されたスクランブルキーが点線で示す経路を経て、ＩＰＭＰツール保持部に送られる。ＩＰＭＰツール保持部では、ライセンスキーを用いてスクランブルキーの解読を行なう。解読されたスクランブルキーは、スクランブルキー保持部で保持され、

ＩＰＭＰツールの動作に使用される。この様に、ＩＰＭＰツールは、スクランブルキーとライセンスキーによる2重のセキュリティがかかっている。

３．　ＩＰＭＰツール用の一般的なインタフェース

データ暗号化／暗号解読、透かし、及び結合透かし及び暗号解読を使用する典型的な用途シナリオを我々が設定した場合、汎用のインタフェースを定義することができる。

データ検出インタフェース

ブロックベースデータ暗号化／暗号解読ツールは、独自のＩＰＭＰシステムにおいてより重要でより広く使用され、特にそのアルゴリズムはある種の収束性を有することが知られている。そこで、そのインタフェースをうまく指定してデータ暗号化及び暗号解読技法の殆どを表すことができ、前記技法の一部は知られていないが、そのインタフェースは予測範囲内である。

データ暗号化／暗号解読の対称アルゴリズム用のＮＥＳＳＩＥインタフェース

あらゆるアクセスユニットのブロックベースデータ暗号化／暗号解読用の汎用インタフェースは、ＩＰＭＰシステムで定義可能である。ＩＰＭＰツールプロバイダとＩＰＭＰ端末実施者の両方は、同一のインタフェースに従って、ツールプロバイダ側でツールをバイナリフォーマットにコンパイルし、ＩＰＭＰ端末側に正しいバイナリツールを伝達することができる。下記のインタフェースは、ＮＥＳＳＩＥ（署名、保全性及び暗号化に関する新欧州方式）で定義されており、我々は、ブロックデータ暗号化／暗号解読用に我々が定義したＩＰＭＰシステムで前記インタフェースに適合することができる。前記インタフェースは、下記のように示され、３種類、ＮＥＳＳＩＥｋｅｙｓｅｔｕｐ（　）、ＮＥＳＳＩＥｅｎｃｒｙｐｔ（　）及びＮＥＳＳＩＥｄｅｃｒｙｐｔ（　）から成る。

```
void NESSIEkeysetup(const unsigned char * const key, struct NESSIEstruct
* const structpointer);
void NESSIEencrypt(const struct NESSIEstruct * const structpointer,
const unsigned char * const plaintext,  unsigned char * const
ciphertext);
void NESSIEdecrypt(const struct NESSIEstruct * const structpointer,
```

const unsigned char * const ciphertext, unsigned char * const plaintext);

透かしインタフェース

透かしを使用する目的に関して、４つの主な分野がある。

・著作権保護――メディアデータの正当な所有権を決定する。

・違法コピー追跡――違法製造コピーを監視して追跡する。

・コピー保護――メディアの許可されていないコピーを禁止する。

・画像認証――データの改造を検出する。

前記分野の各々を分析することにより、次のような事が分かる。著作権保護の場合、符号化側で埋め込みを行い、オフラインで検出を行う。そこでは、他のリアルタイム暗号解読及び復号モジュールと共にＩＰＭＰ端末で実時間実施される必要はない。

コピー保護の場合には、透かしの使用よりも権利認証ツールの方がずっと複雑な使用規則を提供できるので、よりうまく処理可能である。

コンテンツ暗号化及び復号を制御する透かしを使用する場合、透かし検出器は、ＩＰＭＰ端末で指定して実装する必要がある。

たとえ透かしコピー制御埋め込み及び検出にどんなアルゴリズムを使用しても、透かし検出用の汎用インタフェースは、次の通り準拠ＩＰＭＰ端末に関して指定可能である。

ＰＳＬ透かし検出(Unsigned Char* Input, Unsigned Char* WatermarkInfor)

コピー制御をコンテンツプロバイダ／ディストリビュータ側で埋め込み、暗号化及び復号後にコピー制御検出を行うので、上記インタフェースを、ＩＰＭＰ端末で指定して実装することで、異なる透かし検出技法をもＩＰＭＰ端末で使用可能にする必要がある。

画像認証に関して、この場合は著作権保護と同様である。それは、オフラインで行うことができる。

違法コピー追跡用には、他のシステムで広く提案され使用されているコンテンツ追跡の目的でユーザＩＤ又は端末ＩＤを埋め込む透かし埋め込みは優れた機能である。また、基本的な特徴として透かし埋め込みを使用することをここで提案

し、ＩＰＭＰシステムに格納されたり再生用途でコンテンツが違法にコピーされるのを更に防ぐ。ここでＩＰＭＰシステムでは、良く知られているように、最初は保護がデータ暗号化／暗号解読を介して行われ、違法コピーに関する追跡が透かし埋め込みを介して行われる。

たとえ透かし埋め込み、空間定義域又は周波数定義域にどんな技術を使用しても、たとえそれらをどんな分野、映像又は音声に使用しても、入力メッセージ及び出力メッセージは同一であるべきであり、それは次の通りである。

PSLWatermarkEmbedding (Unsigned Char* Input, Unsigned Char* WatermarkInfor, Unsigned Char* Output)

この場合、透かしの検出をオフラインで行うことができる。

どんな種類のアルゴリズムがユーザＩＤ又は端末ＩＤの透かし埋め込みに使用されるかに関しては、ＩＰＭＰ端末実施者の責任である。この場合、準拠ＩＰＭＰ端末が透かし埋め込み機能を実施してＩＤ又は端末ＩＤを埋め込み違法コピーを追跡する必要があるＩＰＭＰシステムで要件を設定する限り、前記インタフェースは、ＩＰＭＰシステムで指定する必要さえもない。

ＩＰＭＰ端末で使用された独立型透かしに関する結論では、汎用インタフェースは透かしを用いたコピー制御検出の場合にのみ定義される。

結合透かし検出及びデータ暗号解読

コンテンツに埋め込まれる暗号解読用キーは、キー自体を処理することによりコンテンツを保護する優れた方法である。このような場合、２つのインタフェースを次の通り指定可能である。

PSLWatermarkExtraction(Unsigned Char* Input, Unsigned Char* Key)

PSLDecryption(Unsigned Char* Input, Unsigned Char* Key, Unsigned Char* Output)

処理は、下記のようである。

ＡＵ用コンテンツ復号→キー抽出→前述のＡＵで抽出されたキーを用いた次のＡＵ暗号解読、循環規則で実行可能である。

４．　部分的データ暗号解読

図８では、データ暗号化及び暗号解読をビットストリーム全体ではなくビット

に適用して選択することができることを示している。

図８（ａ）では、エンコーダを有する部分的暗号化を示しており、コンテンツプロバイダ側で符号化処理中に重要なビットに関して暗号化を選択的に実行できることを説明する。

図８（ａ）において、モジュール８．１は、ＭＰＥＧ２、ＭＰＥＧ４などに基づいて音声又は映像などの元の入力源をストリームに符号化するエンコーダである。モジュール８．２では、選択されたビット又は情報が他のビットの中で必須又は重要であるため、これらのビット又は情報を暗号化してコンテンツを保護する。８．０はスイッチであり、８．８はスイッチ８．０を切りかえるセレクタである。図８（ａ）では、セレクタ８．８は予め決められた周期または時間区分により切り替え信号を出力する。これにより、エンコーダの出力は決められた時間区分において暗号化がかけられ、他の時間は暗号化がなされない。

図８（ｂ）では、エンコーダでエンコードされたデータの内、暗号化を重要なビットに関して選択的に実行できる例を示す。なお、エンコーダ８．１はコンテンツディストリビュータの中にある場合だけでなく、コンテンツディストリビュータの外にある場合も含む。後者の場合であれば、コンテンツディストリビュータは、エンコードされたストリームを受け、それを配信する。これは、コンテンツディストリビュータが既存又はそれら自体の暗号化ツールを用いて符号化コンテンツを保護したい場合である。

図８（ｂ）において、モジュール８．３は、モジュール８．４で実行される暗号化用の重要なビットを構文解析して選択するセレクタを有する部分的デコーダである。エンコードされたストリームは、そのままスイッチ８．０に送られると共に、部分的デコーダおよびセレクタ８．３にも送られる。部分的デコーダおよびセレクタ８．３は、エンコードされたデータをデコードし、重要なデータ部分、たとえば映像信号の場合、Ｉ－ピクチャーの部分やP-ピクチャーの部分を検出する。そして、重要なデータ部分が検出された時に、その部分に対応するエンコードストリームの区分を暗号器８．４に送る様にスイッチ８．０を動作する。このため、エンコーダ８．１からの分岐点とスイッチ８．０との間に必要な遅延部を設けても良い。部分的デコーダおよびセレクタ８．３は、入力されるエンコード

された信号を部分的にデコードしても良いし、全体をデコードしても良い。

図８（ｃ）は、デコード側の構成を示す。ここでは、部分的暗号解読が示されている。ＩＰＭＰ端末側で生じる、部分的暗号化ストリームの暗号解読を選択的に実行する実施の形態を示す。

図８（ｃ）において、モジュール８．５は、モジュール８．６で実行される暗号解読用のビットを構文解析して検出する検出器を有する部分的デコーダである。同時に、復号された音又は画像は、モジュール８．７から出力される。検出器８．５は、デコードを試みることにより、デコードが可能な部分と不可能な部分を検出する。不可能な部分については、その部分に相当するストリームは暗号化されている区分であると判断し、暗号化されている区分を検出する。ストリームの内暗号化されている区分は暗号解読器８．６に送られ、暗号が解読される。

５．　ＩＰＭＰシステム用の可能なプロファイル

異なるアプリケーション、異なる端末、異なるベンダは、ＩＰＭＰシステムに関する異なる要件を有し、たった１つの基準で全部を扱うことは困難である。基本的に、この課題は、ＩＰＭＰツールが事前ロードされるか、又はダウンロード可能であるかに依存する。単純なハードウェア実現に関しては、多くの場合がＪａｖａ仮想マシンを装備しているのである特定のツールがダウンロード可能であるセットトップボックスの新プラットフォームやモバイル装置でさえで多くの場合、殆どのツールは事前ロードされるか、又は組み込まれる。

複雑さの少ない実施を要求する場合にはので、あるモバイル又はポータブル端末は事前符号化ＩＰＭＰツールを有する必要がある。ＰＣアプリケーションは非常に柔軟であり、ツールは、ダウンロード可能又は事前符号化されていてもよい。

ＩＰＭＰツールがダウンロード出来る場合、ダウンロードされたＩＰＭＰツールのインタフェースも、定義される必要がある。メッセージインタフェースは、未知又は専用ＩＰＭＰツールを処理するＩＰＭＰ端末に高い柔軟構造を与える優れた解決策であるが、ＩＰＭＰ端末に対してより複雑な実装を要求する。

３つのプロファイルを指定する場合、表５に示すように端末機能に基づいて３つの場合を扱う。すなわち、固定ＩＰＭＰツール用の単純プロファイル、柔軟ＩＰＭＰツール及び固定インタフェース用のコアプロファイル、並びに柔軟ＩＰＭ

Pツール及び柔軟インタフェース用の高プロファイルの3つである。

【表９】

異なる端末用の３つのプロファイル

プロファイル	IPMP ツール取得	
	事前符号化	ダウンロード済み
単純プロファイル 固定IPMPツール	あり	なし
コアプロファイル 柔軟IPMPツール及び固定インタフェース	あり	あり
高プロファイル 柔軟 IPMP ツール及びインタフェース	あり	あり、より多くのツールを支援できる

ツールが固定される場合は、標準の方法で勧められるＩＰＭＰツールの種類を定義して製造者が端末に実装可能にする必要がある。この場合、インタフェースは、ＩＰＭＰ端末実装者により決定される。

ツールは固定されないがインタフェースが固定される場合に関して、標準の方法で異種のＩＰＭＰツールに関する幾つかの汎用インタフェースを指定する必要がある。

ツールとインタフェースの両方が固定されない場合に関して、メッセージインタフェースを詳細に指定して標準の方法で動作を通知する必要がある。

この発明は、ＩＰＭＰツールリストを構文解析してＩＰＭＰツールを取得するＩＰＭＰツールマネージャモジュールと共にコンテンツストリームの前のＩＰＭＰツールリストパケットを取り入れることにより異種のＩＰＭＰシステムにより同一の保護コンテンツを再生する課題を解決する。ＩＰＭＰツールフォーマットＩＤを指定することにより、異なるフォーマットのＩＰＭＰツールをダウンロードしてＩＰＭＰ端末に一致させることができる。更に、３つの主要なＩＰＭＰツール用の一般的なツールインタフェースも、この発明で指定してＩＰＭＰシステムを完全にする。

２層構造は、より高いセキュリティを与えるだけでなく、異なるユーザ認証方法用の出力構造も固定して、端末互換性を持たせる。このような構造では、ユー

ザ認証を異なるベンダに関して異なる方法で実施して、相互運用性を確保することができる。

異なるプロファイルは、ＩＰＭＰツールを取得して使用する端末複雑性及び柔軟性を考慮して定義され、異なる端末及び異なるＩＰＭＰツールベンダに関して広範囲の適用を与えてながら同一の規準を使用することを可能にする。

図９は、他の実施の一例における著作権保護システムの構成図である。図９において、１はプロバイダ、２はユーザ端末、３はネットワークであり、プロバイダ１とユーザ端末２を接続している。プロバイダ１は、暗号化コンテンツ１１と、その解読鍵１２、及び、著作権保護ツールの一つである解読モジュール１３と、著作権保護情報の一つであるコンテンツの利用規則１４と、その利用規則を管理する著作権保護ツールの一つである利用規則管理モジュール１５を持ち、ユーザ端末２は、初期状態としてなにも持っていない。

以上のように構成された本発明の一実施例における著作権保護（ＩＰＭＰ）システムにおいて、著作権保護システムを更新し、暗号化コンテンツを利用規則に従って解読、再生する方法を以下に述べる。

図１０は、本発明の実施例における著作権保護システムにおいて、プロバイダとユーザ端末の間で交換するメッセージの流れを示す図である。

図１１は、メッセージの具体例であり、各メッセージは、「＝」記号の左辺に示す予め登録されているメッセージ項目名と、「＝」に続くメッセージ項目の値（データ）の組で構成される。

先ず、ユーザ端末２は、視聴したいコンテンツを持つプロバイダにユーザ登録をして必要な著作権保護（ＩＰＭＰ）ツールを入手するためにメッセージ１をプロバイダ１へ送る。メッセージ１は、メッセージ項目として、メッセージＩＤ（識別子）、ユーザ名、支払い方法、及び、ユーザ端末情報より構成される。各メッセージ項目の値は以下である。メッセージ１の目的は、ユーザ登録である為、メッセージＩＤの値は「ユーザ登録」を表わす値であり、登録に必要なユーザ名の値は、「松下　太郎」である。又、視聴するコンテンツの対価の支払い方法の値は、ユーザのクレジットカードの種類、番号、有効期限を含む暗号化された「クレジットカード番号」である。ユーザ端末情報の値は、Windows OS上で動く

マシンであるので「Windows OS」である。

これらの情報は、ネットワーク３の入り口で更に暗号化され、出口でその暗号が解読される。

暗号の方法は、公開鍵暗号方式や共通鍵暗号方式が用いられるが、この内容は、例えば、岡本他「現代暗号」産業図書、１９９７年に詳述されている。

メッセージ１を受け取ったプロバイダは、ユーザ名、解読されたクレジット番号を記録し、ユーザＩＤ「XYZ」をユーザ端末２に割り当て、ユーザ端末２にメッセージ２を返す。メッセージ２は、ユーザがコンテンツを視聴するために必要な初期設定を行うもので、メッセージＩＤの値は、「初期設定」であり、ユーザＩＤの値「XYZ」と、プロバイダが持っているコンテンツの一覧表である「コンテンツリスト」をＩＰＭＰ情報の値として含み、又、暗号化コンテンツを解読する為の解読モジュールの識別子（解読モジュールＩＤ）と、その存在する場所（ロケーション）を、ＩＰＭＰツール情報の値として含む。更に、コンテンツを利用規則に従って視聴させる為、利用規則管理モジュールの識別子（利用規則管理モジュールＩＤ）とその存在する場所（ロケーション）をＩＰＭＰツール情報の値として含む。このとき、解読モジュールと利用規則管理モジュールは、Windowsマシンであるユーザ端末に直接組み込めるものが選ばれる。メッセージ２も、以降のメッセージも、ネットワーク３を通過する際に暗号化されることは、言うまでもない。

メッセージ２を受け取ったユーザ端末は、解読モジュールＩＤとそのロケーションで指定される解読モジュールと、同じく利用規則管理モジュールＩＤとそのロケーションで指定される利用規則管理モジュールを、ファイル転送などの手段で入手し、自身に著作権保護ツール（ＩＰＭＰツール）として組み込む。このファイル転送も又、暗号化されたファイル転送であり、他のユーザ端末は暗号解読の鍵を持たない為、モジュールを傍受したとしても解読できない。

次に、ユーザ端末２は、コンテンツリストから視聴を希望するコンテンツ１を選び、コンテンツ要求をメッセージＩＤとして持つメッセージ３をプロバイダに送る。メッセージ３は、更に、ユーザＩＤとして値「XYZ」を含み、コンテンツ情報として要求するコンテンツ１のＩＤを含む。

これを受けたプロバイダ１は、要求されたコンテンツ１の対価を、ユーザのクレジットカード番号を使ってクレジットカード会社に請求した後、暗号化コンテンツ１をユーザ端末２に送る為、メッセージ４を返す。メッセージ４は、メッセージＩＤと、２つの著作権保護（ＩＰＭＰ）情報、及びコンテンツ情報で構成される。メッセージＩＤの値は「コンテンツ配信」であり、ＩＰＭＰ情報の値は、要求されたコンテンツ１の利用規則１と、暗号化されたコンテンツ１の暗号を解く為の解読鍵１である。コンテンツ情報は、要求された暗号化コンテンツ１そのものである。解読鍵１は、公開鍵暗号方式で暗号化されてユーザ端末２に送られるので、このメッセージ４を第三者が傍受しても解読鍵の暗号を解読出来ず、コンテンツの漏洩は起こらない。

メッセージ４を受け取ったユーザ端末２では、先ほど組み込んだ利用規則管理モジュール２５が、利用規則１を確認しながら、解読モジュール２３を制御し、解読モジュール２３は、解読鍵１を使って、暗号化コンテンツ１を解読し、解読されたコンテンツ１を表示出力する。解読モジュール２３が暗号化コンテンツ１の暗号を解く動作は、共通鍵暗号方式であり、上述の文献に詳しく述べられている。

次に、図１２に示す利用規則１の一実施例に従い、暗号化コンテンツ１の解読を行う解読モジュール２３を制御する利用規則管理モジュール２５の動作を、図１３のフロー図を用いて以下に説明する。

先ず、利用規則管理モジュール２５は、利用規則１の第1行目を調べ、このコンテンツが利用可能期間内に入っているか否かを、ユーザ端末の持つ時計で確認し、入っていなければ、処理を終了する。

入っていれば次に、ユーザにこのコンテンツを別メモリに移動するか否かを確認し、移動する場合は、利用規則1内の移動可能回数を調べ、この値がゼロより大であれば、ユーザの指定するメモリにコンテンツを移動し、移動可能回数を１減じる。

次に、ユーザにこのコンテンツのコピーを作るか否かを確認し、作る場合は、利用規則1内のコピー可能回数を調べ、この値がゼロより大であれば、ユーザの指定するメモリにコンテンツとその利用規則をコピーし、コピー可能回数を１減

じる。コピー先のコンテンツのコピー可能回数は、処理の簡単化のためにゼロとするが、トータルのコピー回数が初期のコピー可能回数を越えない様に制御しても良い。

次に、ユーザにこのコンテンツを再生するか否かを確認し、再生する場合は、利用規則1内の再生可能回数を調べ、この値がゼロより大であれば、解読モジュール２３にコンテンツの解読・表示出力を指令する。

指令を受けた解読モジュール２３は、コンテンツ１の暗号解読を行いその結果を表示出力することは上述の通りである。

次に、利用規則管理モジュール２５は、再生終了を検出し、それまでに再生した時間が無料再生時間を超過したか否かを調べ、超過した場合は、再生可能回数を１減じて終了する。

以上に述べた利用規則管理モジュール２５による利用規則１の管理により、プロバイダ１が意図した回数の再生のみが実行される。同時に、コピー回数や、移動回数もプロバイダの意図どおりに管理される。

尚、本実施例では、メッセージは、予め決められたメッセージ項目と「＝」で結ばれたその項目の値（データ）との組で構成されていたが、メッセージの値の意味が分かる方法であれば何でも良く、例えば、メッセージ中のビットの位置に予め決められた意味を割り当てる方法でも良い。

以上のような構成及び方法により、本発明の更新可能な著作権保護システムでは、プロバイダからユーザ端末に送られるメッセージをユーザ端末が解読することにより、著作権保護モジュールの更新と、プロバイダが与える利用規則に従ったコンテンツの視聴が可能となる。

すなわち、メッセージ中にモジュールＩＤが存在するかしないかで、モジュールの更新を行うか否かが判定でき、モジュールＩＤが存在する場合はロケーションの値で、どこにモジュールがあるかが分かり、モジュールのダウンロードが可能となる。

又、メッセージ項目名が予め決められているので、このメッセージ項目名を探すことで、メッセージ項目の値を得られるので、メッセージ項目とその値の組はメッセージ中にどの順番で入っていても良い。

又、上記の様に、プロバイダ１は、メッセージ１でユーザ端末２のOSの種類を知り、そのユーザ端末２に適合する著作権保護モジュール１を選んで、ユーザ端末２にダウンロードすることにより、ユーザ端末２は、仮想マシンを実装する必要はない。

請　求　の　範　囲

1．　符号化技術を用いてコンテンツをコンテンツストリームに符号化する手段と、

データ暗号化ツールを用いて当該符号化コンテンツストリームを暗号化する手段と、

透かしツールを用いて当該コンテンツに透かし情報を埋め込む手段と、

上記ステップで用いられた当該コンテンツに関するコンテンツＩＤ及びＩＰＭＰ（知的所有権管理保護）ツールリスト（ＩＰＭＰツール情報）を作成する手段と、

各コンテンツストリームのヘッダとして保持すべきＩＰＭＰツールリストフラグを作成する手段と、

ＩＰＭＰツールリストフラグ、次いでＩＰＭＰツールリスト、コンテンツＩＤ及び実際の符号化コンテンツストリームを含むコンテンツストリームを構成する手段と、

を含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟及び共通ＩＰＭＰシステムの装置。

2．　符号化技術を用いてコンテンツをコンテンツストリームに符号化する手段と、

データ暗号化ツール又は他のツールを用いた当該符号化コンテンツストリームを暗号化する手段と、

上記ステップで用いられた当該コンテンツに関するコンテンツＩＤ及びＩＰＭＰ（知的所有権管理保護）ツールリスト（ＩＰＭＰツール情報）を作成する手段と、

各コンテンツストリームのヘッダとして保持すべきＩＰＭＰツールリストフラグを作成する手段と、

ＩＰＭＰツールリストフラグ、次いでＩＰＭＰツールリスト、コンテンツＩＤ及び実際の符号化コンテンツストリームを含むコンテンツストリームを構成する手段と、

を含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟及び共通ＩＰＭＰシステムの装置。

３．　符号化技術を用いてコンテンツをコンテンツストリームに符号化する手段と、

暗号化キーを有する暗号化ツール又は他のツールを用いて当該コンテンツストリームを暗号化する手段と、

より高いセキュリティのために別の暗号化キーを有する任意の暗号化ツールを用いて当該暗号化キーを暗号化する手段と、

当該コンテンツストリームと同一のストリームに保持されたＩＰＭＰ情報に上記当該暗号化されたキーを埋め込む手段と、

上記ステップで使われた当該コンテンツに関するコンテンツＩＤ及びＩＰＭＰ（知的所有権管理保護）ツールリスト（ＩＰＭＰツール情報）を作成する手段と、

各コンテンツストリームのヘッダとして保持すべきＩＰＭＰツールリストフラグを作成する手段と、

ＩＰＭＰツールリストフラグ、次いでＩＰＭＰツールリスト、コンテンツＩＤ及び実際の符号化コンテンツストリームを含むコンテンツストリームを構成する手段と、

を含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟ＩＰＭＰシステムの装置。

４．　請求項１、２及び３において当該コンテンツに関するコンテンツＩＤ及びＩＰＭＰツールリストを作成することが、

ＩＰＭＰツールＩＤを各コンテンツに割当てて、何れのツールをデータ保護に使用するかを表示する手段と、

位置タイプＩＤを各ＩＰＭＰツールに割当てて、当該ＩＰＭＰツールが入手可能である位置のタイプを通知する手段と、

フォーマットＩＤを割当てて、ダウンロードされたＩＰＭＰツールフォーマットを表示して、準拠ＩＰＭＰ端末がそれらのプラットフォームに基づいて選択及び検索することを可能にする手段と、

当該ＩＰＭＰツールの位置を表示して、端末が当該ＩＰＭＰツールを当該位置

から取得することを可能にする手段と、

を更に含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟ＩＰＭＰシステムの装置。

５．　ＩＰＭＰ端末のＩＰＭＰツールマネージャでコンテンツストリームの中を構文解析する手段と、

ＩＰＭＰツールリストフラグ、コンテンツＩＤ及びＩＰＭＰツールリストを解釈する手段と、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該ＩＰＭＰツールリストに基づいてＩＰＭＰツールを取得する手段と、

を含む、ＩＰＭＰ端末側のコンテンツ提供及び保護用の柔軟ＩＰＭＰシステムの装置。

６．　ＩＰＭＰ端末のＩＰＭＰツールマネージャでコンテンツストリームの中を構文解析する手段と、

ＩＰＭＰツールリストフラグ、コンテンツＩＤ及びＩＰＭＰツールリストを解釈する手段と、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該ＩＰＭＰツールリストに基づいてＩＰＭＰツールを取得する手段と、

要求をコンテンツディストリビュータに自動的に出して、ユーザ権利認証を行う手段と、

前記ユーザ権利認証が成功した後、当該コンテンツディストリビュータからライセンス又はキー情報を受信する手段と、

前記ユーザ権利認証が成功した後、要求されたコンテンツの消費用の使用規則を取得する手段と、

を含む、ＩＰＭＰ端末側のコンテンツ提供及び保護用の柔軟及び共通ＩＰＭＰシステムの装置。

７．　要求をコンテンツディストリビュータに自動的に出して、ユーザ権利認証を行う手段と、

前記ユーザ権利認証が成功した後、当該コンテンツディストリビュータからライセンス又はキー情報を受信する手段と、

当該ライセンス又はキー情報をＩＰＭＰ端末で構文解析する手段と、

当該ライセンス又はキー情報を当該ＩＰＭＰ端末のメモリに格納する手段と、

当該ＩＰＭＰ端末のＩＰＭＰツールマネージャでコンテンツストリームの中を構文解析する手段と、

ＩＰＭＰツールリストフラグ、コンテンツＩＤ及びＩＰＭＰツールリストを解釈する手段と、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該ＩＰＭＰツールリストに基づいてＩＰＭＰツールを取得する手段と、

ＩＰＭＰツールリスト情報の当該部分と共に上記ステップで検索された当該ＩＰＭＰツールを当該ＩＰＭＰ端末のメモリに格納する手段と、

当該メモリに格納された当該ＩＰＭＰツールと共に当該ライセンス／キー情報を用いて当該コンテンツストリームを暗号解読及び復号する手段と、

を含む、ＩＰＭＰ端末側のコンテンツ提供及び保護用の柔軟及び共通ＩＰＭＰシステムの装置。

８．　要求をコンテンツディストリビュータに送信して、ユーザ認証を行う手段と、

当該コンテンツディストリビュータからライセンス又はキー情報を受信する手段と、

当該ライセンス又はキー情報をＩＰＭＰ端末で構文解析する手段と、

当該ライセンス又はキー情報を当該ＩＰＭＰ端末のメモリに格納する手段と、

当該ＩＰＭＰ端末のＩＰＭＰツールマネージャでコンテンツストリームの中を構文解析する手段と、

ＩＰＭＰツールリストフラグ、コンテンツＩＤ及びＩＰＭＰツールリストを解釈する手段と、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該ＩＰＭＰツールリストに基づいてＩＰＭＰツールを取得

する手段と、

ＩＰＭＰツールリスト情報の当該部分と共に上記ステップで検索された当該ＩＰＭＰツールを当該ＩＰＭＰ端末のメモリに格納する手段と、

当該ライセンス又はキー情報を用いて当該ＩＰＭＰ情報内の当該暗号化されたキーを暗号解読する手段と、

コンテンツプロバイダ側で当該コンテンツを暗号化するために使用された暗号化キーを上記ステップから取得する手段と、

上記ステップから取得された当該暗号化キーを用いて当該コンテンツを暗号解読して、最初のコンテンツを取得する手段と、

当該最初のコンテンツを当該ＩＰＭＰ端末での再生のために復号する手段と、

を含む、ＩＰＭＰ端末側のコンテンツ提供及び保護用の柔軟及び共通ＩＰＭＰシステムの装置。

９．　請求項５、６、７、８のいずれかにおいてＩＰＭＰツールリストは、

ＩＰＭＰツールの大部分に関するＩＰＭＰツールＩＤをテーブル状に定義しており、

当該テーブルに予約可能な未使用スペースがあり、

ＩＰＭＰツールタイプとも呼ばれるＩＰＭＰツールのカテゴリとしてＩＰＭＰツールＩＤの一部が定義されており、

当該テーブルをＩＰＭＰ端末に事前ロード、事前符号化又はダウンロードする手段と、

前記コンテンツストリーム内に保持された当該ＩＰＭＰツールリストから当該ＩＰＭＰツールＩＤを抽出する手段と、

前記コンテンツストリームに保持された当該ＩＰＭＰツールリストに表示されたＩＰＭＰツール位置識別子を取得する手段と、

ＩＰＭＰツール位置識別子に加えて、ＩＰＭＰツールＩＤと共に、当該コンテンツストリームに保持されたＩＰＭＰツールフォーマットＩＤを取得する手段と、

適切なフォーマットであるＩＰＭＰツールを選択して、ＩＰＭＰ端末プラットフォームに適合させる手段と、

上記手段で取得された当該位置から当該ＩＰＭＰツールを検索する手段と、

とを更に含む、ＩＰＭＰ端末側のコンテンツ提供及び保護用の柔軟及び共通ＩＰＭＰシステムの装置。

１０．　予め定めたテーブルに基づいてＩＰＭＰツールリストを構築してコンテンツに使用されたＩＰＭＰツールの内容をＩＰＭＰ端末に通知することが、

データ暗号解読、透かしなどのＩＰＭＰツールのカテゴリとして当該予め定めたテーブルからＩＰＭＰツールタイプＩＤを選択する手段と、

当該ＩＰＭＰツールタイプＩＤの下である特定のアルゴリズムを有するある特定のＩＰＭＰツールに関して当該予め定めたテーブルからＩＰＭＰツールＩＤを選択する手段と、

当該予め定めたテーブルからＩＰＭＰツール位置ＩＤを選択して、ＩＰＭＰツールをダウンロード又は検索可能な場所を通知する手段と、

ＩＰＭＰツールを遠隔で検索する場合、当該ＩＰＭＰツールリストにＵＲＬ位置を与える手段と、

バイナリフォーマットにプリコンパイルされたＩＰＭＰツールの各セットに関するＩＰＭＰツールフォーマットＩＤを選択する手段と、

を更に含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟及び共通ＩＰＭＰシステムの装置。

１１．　請求項１、２、３のいずれかにおいて暗号化ツールを用いて事前符号化コンテンツストリームを暗号化することが、

イントラ符号化フレーム（Ｉフレーム）などの事前符号化映像ストリームでキーアクセスユニットを探索する手段と、

ずべてのアクセスユニットを暗号化する代わりに暗号化ツールを用いて当該キーアクセスユニットのみを暗号化して、暗号解読側の処理を高速化する手段と、

を更に含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟及び共通ＩＰＭＰシステムの装置。

１２．　請求項１、２、３のいずれかにおいて暗号化ツールを用いて事前符号化コンテンツストリームを暗号化することが、

事前符号化映像ストリーム又は音声ストリームで重要ビットを探索する手段と、

ずべてのアクセスユニットを暗号化する代わりに暗号化ツールを用いて当該重

要ビットのみを暗号化して、暗号解読側の処理を高速化する手段と、

を更に含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟及び共通ＩＰＭＰシステムの装置。

１３．　請求項１１または１２において選択されたアクセスユニット又は重要ビットに関して暗号化を部分的に行われた保護コンテンツストリームを復号する手段と、

予め定めた規則に基づいて暗号化されたビット又はアクセスユニットを探索して、所与のデータ暗号解読ツールを用いて前記ビット又はアクセスユニットを暗号解読する手段と、

を含む、保護コンテンツを暗号解読して再生するＩＰＭＰ端末側のコンテンツ提供及び保護用の柔軟及び共通ＩＰＭＰシステムの装置。

１４．　指定インタフェースに従ってＩＰＭＰツールがされており、

当該インタフェースを含んだＩＰＭＰ端末が構築されたＩＰＭＰシステムの装置において、

当該ＩＰＭＰツールを検索して当該端末の当該インタフェースに適合させる手段

を含む、コンテンツ提供及び保護用の柔軟及び共通ＩＰＭＰシステムの装置。

１５．　ＭＰＥＧ－４システムにある基本ストリームに対応付けられたデコーダ構成記述子に新しいストリームタイプを指定し、

ＭＰＥＧ－４のＩＰＭＰ基本ストリームにＩＰＭＰツールを保持することを可能にした、コンテンツ提供及び保護用の柔軟及び共通ＩＰＭＰシステムの装置。

１６．　符号化技術を用いてコンテンツをコンテンツストリームに符号化するステップと、

データ暗号化ツールを用いて当該符号化コンテンツストリームを暗号化するステップと、

透かしツールを用いて当該コンテンツに透かし情報を埋め込むステップと、

上記ステップで用いられた当該コンテンツに関するコンテンツＩＤ及びＩＰＭＰ（知的所有権管理保護）ツールリスト（ＩＰＭＰツール情報）を作成するステ

ップと、

各コンテンツストリームのヘッダとして保持すべきＩＰＭＰツールリストフラグを作成するステップと、

ＩＰＭＰツールリストフラグ、次いでＩＰＭＰツールリスト、コンテンツＩＤ及び実際の符号化コンテンツストリームを含むコンテンツストリームを構成するステップと、

を含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟及び共通ＩＰＭＰシステムの方法。

１７．　符号化技術を用いてコンテンツをコンテンツストリームに符号化するステップと、

データ暗号化ツール又は他のツールを用いて当該符号化コンテンツストリームを暗号化するステップと、

上記ステップで用いた当該コンテンツに関するコンテンツＩＤ及びＩＰＭＰ（知的所有権管理保護）ツールリスト（ＩＰＭＰツール情報）を作成するステップと、

各コンテンツストリームのヘッダとして保持すべきＩＰＭＰツールリストフラグを作成するステップと、

ＩＰＭＰツールリストフラグ、次いでＩＰＭＰツールリスト、コンテンツＩＤ及び実際の符号化コンテンツストリームを含むコンテンツストリームを構成するステップと、

を含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟及び共通ＩＰＭＰシステムの方法。

１８．　符号化技術を用いてコンテンツをコンテンツストリームに符号化するステップと、

暗号化キーを有する暗号化ツール又は他のツールを用いて当該コンテンツストリームを暗号化するステップと、

より高いセキュリティのために別の暗号化キーを有する任意の暗号化ツールを用いて当該暗号化キーを暗号化するステップと、

当該コンテンツストリームと同一のストリームに保持されたＩＰＭＰ情報に上

記当該暗号化されたキーを埋め込むステップと、

上記ステップで用いた当該コンテンツに関するコンテンツＩＤ及びＩＰＭＰ（知的所有権管理保護）ツールリスト（ＩＰＭＰツール情報）を作成するステップと、

各コンテンツストリームのヘッダとして保持すべきＩＰＭＰツールリストフラグを作成するステップと、

ＩＰＭＰツールリストフラグ、次いでＩＰＭＰツールリスト、コンテンツＩＤ及び実際の符号化コンテンツストリームを含むコンテンツストリームを構成するステップと、

を含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟ＩＰＭＰシステムの方法。

１９．　請求項１６、１７、１８のいずれかにおいて当該コンテンツに関するコンテンツＩＤ及びＩＰＭＰツールリストを作成することが、

ＩＰＭＰツールＩＤを各コンテンツに割当てて、何れのツールをデータ保護に使用するかを表示するステップと、

位置タイプＩＤを各ＩＰＭＰツールに割当てて、当該ＩＰＭＰツールが入手可能である位置のタイプを通知するステップと、

フォーマットＩＤを割当てて、ダウンロードされたＩＰＭＰツールフォーマットを表示して、準拠ＩＰＭＰ端末がそれらのプラットフォームに基づいて選択及び検索することを可能にするステップと、

当該ＩＰＭＰツールの位置を表示して、端末が当該ＩＰＭＰツールを当該位置から取得することを可能にするステップと、

を更に含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟ＩＰＭＰシステムの方法。

２０．　ＩＰＭＰ端末のＩＰＭＰツールマネージャでコンテンツストリームの中を構文解析するステップと、

ＩＰＭＰツールリストフラグ、コンテンツＩＤ及びＩＰＭＰツールリストを解釈するステップと、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテ

ンツストリームから当該ＩＰＭＰツールリストに基づいてＩＰＭＰツールを取得するステップと、

を含む、ＩＰＭＰ端末側のコンテンツ提供及び保護用の柔軟ＩＰＭＰシステムの方法。

２１．　ＩＰＭＰ端末のＩＰＭＰツールマネージャでコンテンツストリームの中を構文解析するステップと、

ＩＰＭＰツールリストフラグ、コンテンツＩＤ及びＩＰＭＰツールリストを解釈するステップと、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該ＩＰＭＰツールリストに基づいてＩＰＭＰツールを取得するステップと、

要求をコンテンツディストリビュータに自動的に出して、ユーザ権利認証を行うステップと、

前記ユーザ権利認証が成功した後、当該コンテンツディストリビュータからライセンス又はキー情報を受信するステップと、

前記ユーザ権利認証が成功した後、要求されたコンテンツの消費用の使用規則を取得するステップと、

を含む、ＩＰＭＰ端末側のコンテンツ提供及び保護用の柔軟及び共通ＩＰＭＰシステムの方法。

２２．　要求をコンテンツディストリビュータに自動的に出して、ユーザ権利認証を行うステップと、

前記ユーザ権利認証が成功した後、当該コンテンツディストリビュータからライセンス又はキー情報を受信するステップと、

当該ライセンス又はキー情報をＩＰＭＰ端末で構文解析するステップと、

当該ライセンス又はキー情報を当該ＩＰＭＰ端末のメモリに格納するステップと、

当該ＩＰＭＰ端末のＩＰＭＰツールマネージャでコンテンツストリームの中を構文解析するステップと、

ＩＰＭＰツールリストフラグ、コンテンツＩＤ及びＩＰＭＰツールリストを解

釈するステップと、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該ＩＰＭＰツールリストに基づいてＩＰＭＰツールを取得するステップと、

ＩＰＭＰツールリスト情報の当該部分と共に上記ステップで検索された当該ＩＰＭＰツールを当該ＩＰＭＰ端末のメモリに格納するステップと、

当該メモリに格納された当該ＩＰＭＰツールと共に当該ライセンス／キー情報を用いて当該コンテンツストリームを暗号解読及び復号するステップと、

を含む、ＩＰＭＰ端末側のコンテンツ提供及び保護用の柔軟及び共通ＩＰＭＰシステムの方法。

２３．　要求をコンテンツディストリビュータに送信して、ユーザ認証を行うステップと、

当該コンテンツディストリビュータからライセンス又はキー情報を受信するステップと、

当該ライセンス又はキー情報をＩＰＭＰ端末で構文解析するステップと、

当該ライセンス又はキー情報を当該ＩＰＭＰ端末のメモリに格納するステップと、

当該ＩＰＭＰ端末のＩＰＭＰツールマネージャでコンテンツストリームの中を構文解析するステップと、

ＩＰＭＰツールリストフラグ、コンテンツＩＤ及びＩＰＭＰツールリストを解釈するステップと、

ローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該ＩＰＭＰツールリストに基づいてＩＰＭＰツールを取得するステップと、

ＩＰＭＰツールリスト情報の当該部分と共に上記ステップで検索された当該ＩＰＭＰツールを当該ＩＰＭＰ端末のメモリに格納するステップと、

当該ライセンス又はキー情報を用いて当該ＩＰＭＰ情報内の当該暗号化されたキーを暗号解読するステップと、

コンテンツプロバイダ側で当該コンテンツを上記ステップで暗号化するために

使用された暗号化キーを取得するステップと、

上記ステップから取得された当該暗号化キーを用いて当該コンテンツを暗号解読して、最初のコンテンツを取得するステップと、

当該最初のコンテンツを当該ＩＰＭＰ端末で再生する為に復号するステップと、

を含む、ＩＰＭＰ端末側のコンテンツ提供及び保護用の柔軟及び共通ＩＰＭＰシステムの方法。

２４．　請求項２０、２１、２２、２３のいずれかにおいてローカル（事前ロード又は事前符号化）、周辺装置、遠隔側、又は当該コンテンツストリームから当該ＩＰＭＰツールリストに基づいてＩＰＭＰツールを取得することが、

ＩＰＭＰツールの大部分に関するＩＰＭＰツールＩＤをテーブルに定義されており、

今後の又は未知／専用のＩＰＭＰツールに使用されるべきＩＰＭＰツールＩＤに関する項目を当該テーブルに予約する余地があり、

ＩＰＭＰツールタイプとも呼ばれるＩＰＭＰツールのカテゴリとしてＩＰＭＰツールＩＤの一部が定義されている、

当該テーブルをＩＰＭＰ端末に事前ロード、事前符号化又はダウンロードするステップと、

前記コンテンツストリーム内に保持された当該ＩＰＭＰツールリストから当該ＩＰＭＰツールＩＤを抽出するステップと、

前記コンテンツストリームに保持された当該ＩＰＭＰツールリストに表示されたＩＰＭＰツール位置識別子を取得するステップと、

ＩＰＭＰツール位置識別子に加えて、ＩＰＭＰツールＩＤと共に、当該コンテンツストリームに保持されたＩＰＭＰツールフォーマットＩＤを取得するステップと、

適切なフォーマットであるＩＰＭＰツールを選択して、ＩＰＭＰ端末プラットフォームに適合させるステップと、

上記手段で取得された当該位置から当該ＩＰＭＰツールを検索するステップと、

を更に含む、ＩＰＭＰ端末側のコンテンツ提供及び保護用の柔軟及び共通ＩＰＭＰシステムの方法。

２５．　予め定めたテーブルに基づいてＩＰＭＰツールリストを構築して、コンテンツに使用されたＩＰＭＰツールの内容をＩＰＭＰ端末に通知するステップと、

対応するコンテンツストリームの前に当該ＩＰＭＰツールリストを挿入するステップと、

を含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟及び共通ＩＰＭＰシステムの方法。

２６．　予め定めたテーブルに基づいてＩＰＭＰツールリストを構築してコンテンツに使用されたＩＰＭＰツールの内容をＩＰＭＰ端末に通知することが、

データ暗号解読、透かしなどのＩＰＭＰツールのカテゴリとして当該予め定めたテーブルからＩＰＭＰツールタイプＩＤを選択するステップと、

当該ＩＰＭＰツールタイプＩＤの下である特定のアルゴリズムを有するある特定のＩＰＭＰツールに関して当該予め定めたテーブルからＩＰＭＰツールＩＤを選択するステップと、

当該予め定めたテーブルからＩＰＭＰツール位置ＩＤを選択して、ＩＰＭＰツールをダウンロード又は検索可能な場所を通知するステップと、

ＩＰＭＰツールを遠隔で検索する場合、当該ＩＰＭＰツールリストにＵＲＬ位置を与えるステップと、

バイナリフォーマットにプリコンパイルされたＩＰＭＰツールの各セットに関するＩＰＭＰツールフォーマットＩＤを選択するステップと、

を更に含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟及び共通ＩＰＭＰシステムの方法。

２７．　請求項１６、１７、１８のいずれかにおいて暗号化ツールを用いて事前符号化コンテンツストリームを暗号化することが、

イントラ符号化フレーム（Ｉフレーム）などの事前符号化映像ストリームでキーアクセスユニットを探索するステップと、

ずべてのアクセスユニットを暗号化する代わりに暗号化ツールを用いて当該キーアクセスユニットのみを暗号化して、暗号解読側の処理を高速化するステップと、

を更に含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟及び共

通ＩＰＭＰシステムの方法。

２８．　請求項１６、１７、１８のいずれかにおいて暗号化ツールを用いて事前符号化コンテンツストリームを暗号化することが、

事前符号化映像ストリーム又は音声ストリームで重要ビットを探索するステップと、

ずべてのアクセスユニットを暗号化する代わりに暗号化ツールを用いて当該重要ビットのみを暗号化して、暗号解読側の処理を高速化するステップと、

を更に含む、コンテンツプロバイダ側のコンテンツ提供及び保護用の柔軟及び共通ＩＰＭＰシステムの方法。

２９．　請求項２７または２８において選択されたアクセスユニット又は重要ビットに関して暗号化を部分的に行うことが、

保護コンテンツストリームを復号するステップと、

予め定めた規則に基づいて暗号化されたビット又はアクセスユニットを探索して、所与のデータ暗号解読ツールを用いて前記ビット又はアクセスユニットを暗号解読するステップと、

を含む、保護コンテンツを暗号解読して再生するＩＰＭＰ端末側のコンテンツ提供及び保護用の柔軟及び共通ＩＰＭＰシステムの方法。

３０．　ＭＰＥＧ－４システムにある基本ストリームに対応付けられたデコーダ構成記述子に新しいストリームタイプを指定して、

ＭＰＥＧ－４のＩＰＭＰ基本ストリームにＩＰＭＰツールを保持することを可能にした、コンテンツ提供及び保護用の柔軟及び共通ＩＰＭＰシステムの方法。

３１．　暗号化されたコンテンツと、その解読鍵と、解読モジュールと、コンテンツの利用規則と、利用規則管理モジュールを持つプロバイダと、ネットワークを通じて接続されたユーザ端末から構成され、プロバイダ側で、ユーザ端末に送るメッセージ中に、更新すべきソフトウエアモジュールの識別子とその存在する場所を示す情報を含めることにより、ユーザ端末に著作権保護システムの更新を行わせ、更新すべきソフトウエアモジュールは、解読モジュールと利用規則管理モジュールを含むことにより、プロバイダの意図する利用規則に従ってコンテンツの解読・視聴を行うことを特徴とするコンテンツ提供及び保護用の柔軟及び変

通ＩＰＭＰシステムの装置。

３２．　暗号化されたコンテンツと、その解読鍵と、解読モジュールと、コンテンツの利用規則と、利用規則管理モジュールを持つプロバイダと、ネットワークを通じて接続されたユーザ端末から構成され、ユーザ端末は、プロバイダから利用規則管理モジュールを受け取って自身に組み込み、これを用いて、プロバイダから受け取る著作権保護情報の中にある、コンテンツの利用規則に従い、プロバイダから受け取るコンテンツの再生を行うことを特徴とするコンテンツ提供及び保護用の柔軟及び変通ＩＰＭＰシステムの装置。

３３．　利用規則は、コンテンツの利用可能期間、無料再生可能時間、再生可能回数、コピー可能回数、移動可能回数のいずれかを含むことを特徴とする請求項３１または３２に記載のコンテンツ提供及び保護用の柔軟及び変通ＩＰＭＰシステムの装置。

３４．　プロバイダからユーザ端末に送られるメッセージは、メッセージ項目名と直後に続くメッセージ項目の値の組で構成され、ユーザ端末に送るメッセージ項目の順序を問わないことを特徴とする、請求項３１または３２に記載のコンテンツ提供及び保護用の柔軟及び変通ＩＰＭＰシステムの装置。

３５．　ユーザ端末からプロバイダに送られるメッセージは、ユーザ端末情報を含むことにより、ユーザ端末に適合するモジュールをプロバイダから受信することが出来ることを特徴とする請求項３１または３２に記載のコンテンツ提供及び保護用の柔軟及び変通ＩＰＭＰシステムの装置。

Fig.1

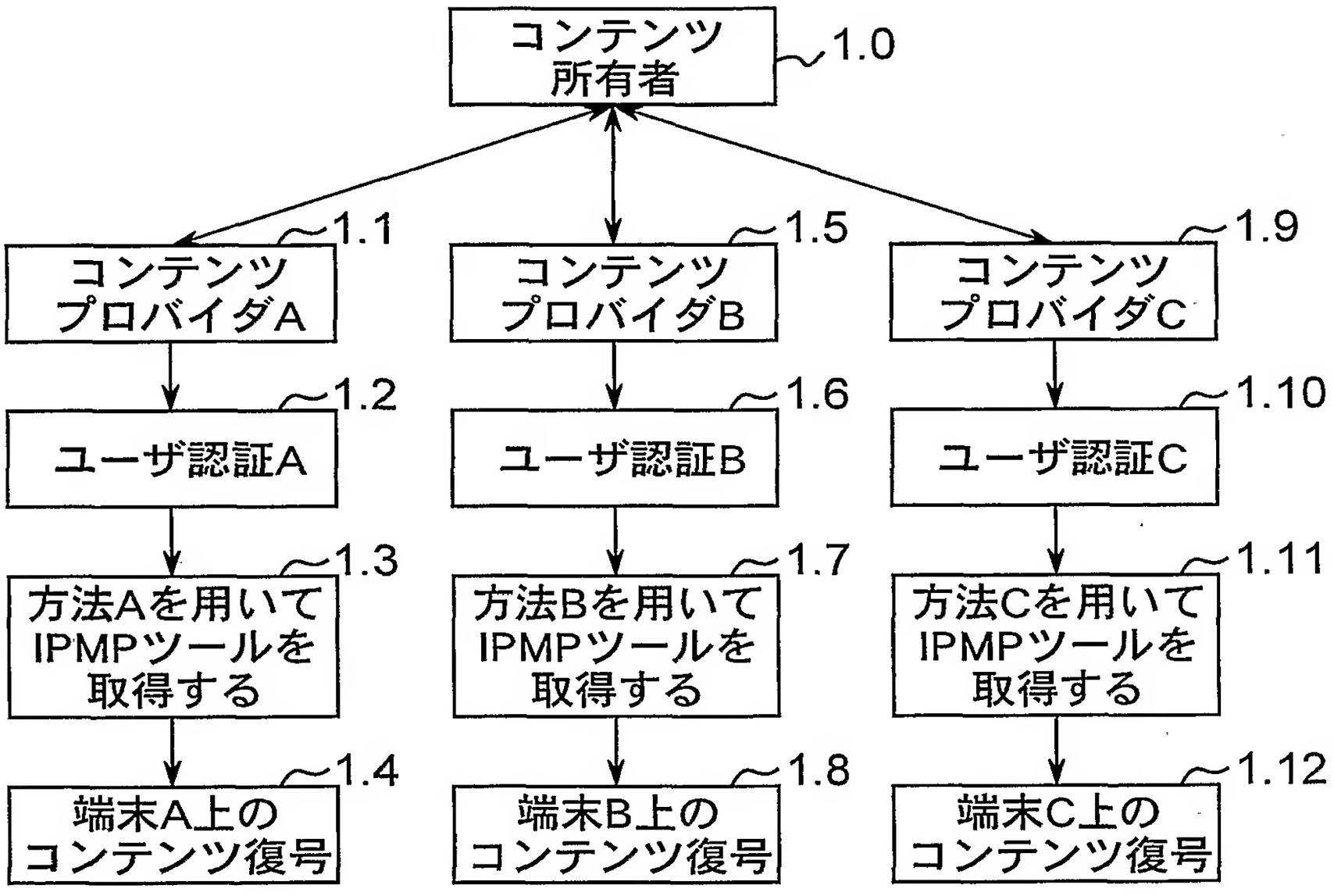
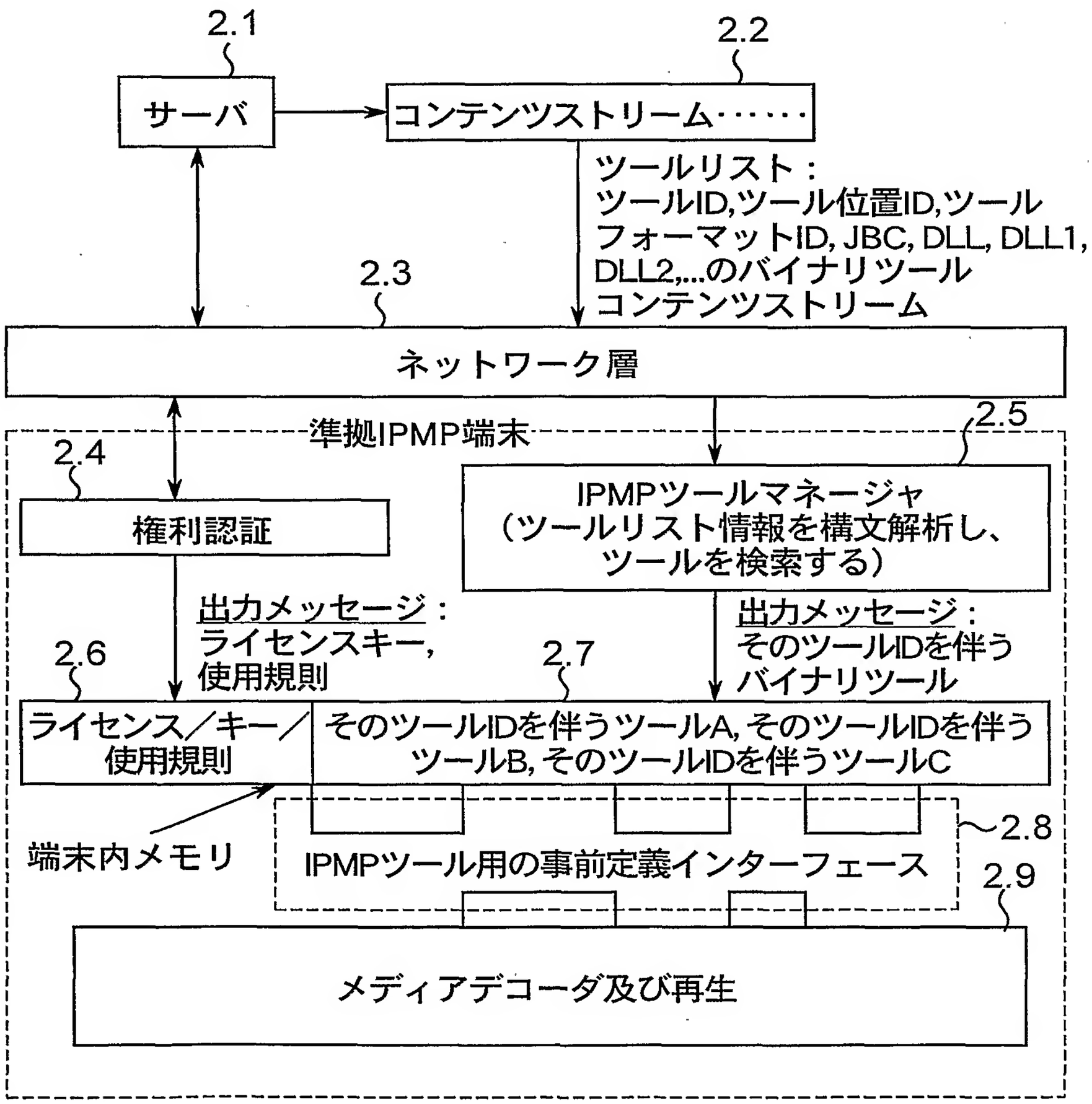


Fig.2



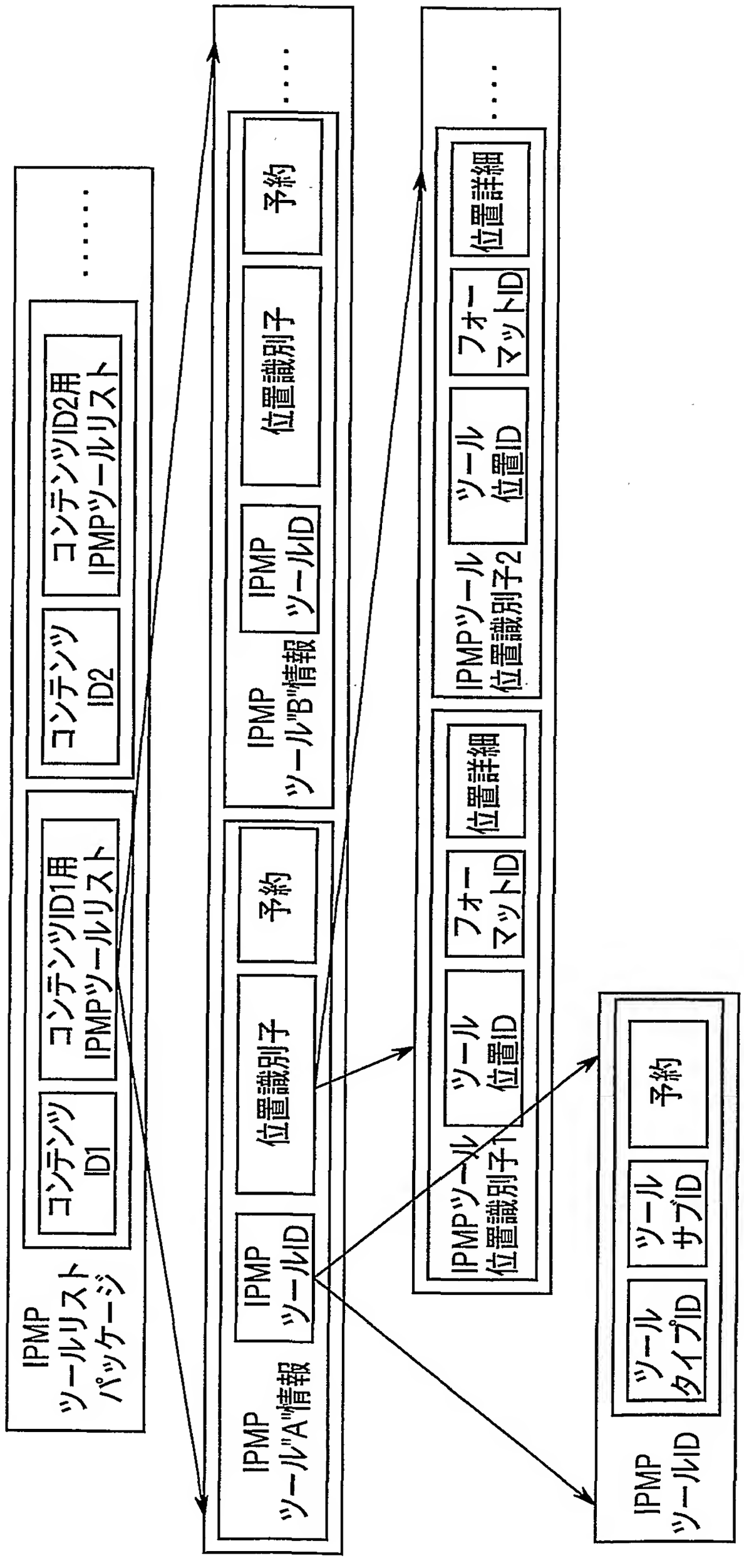


Fig.3

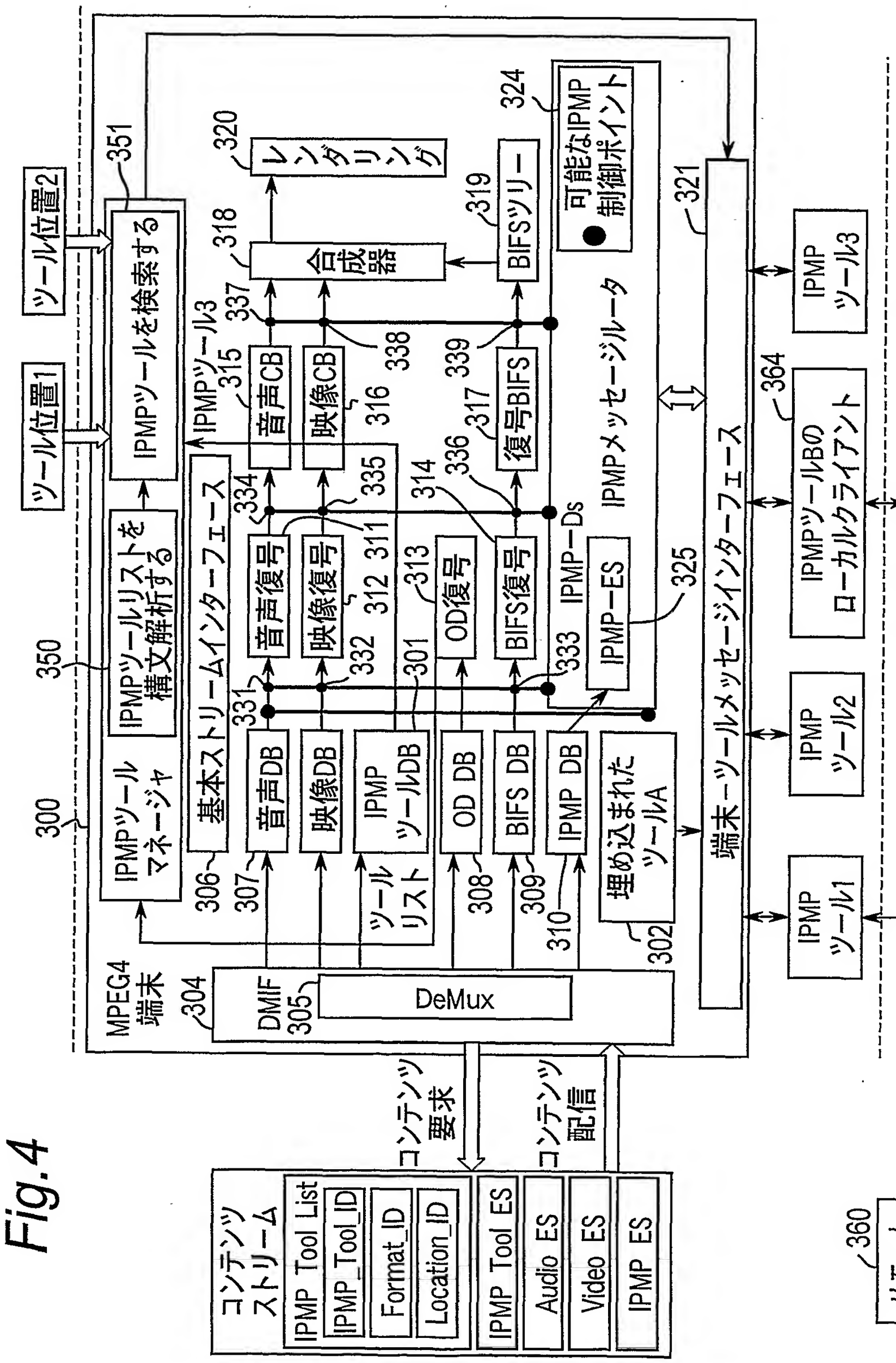
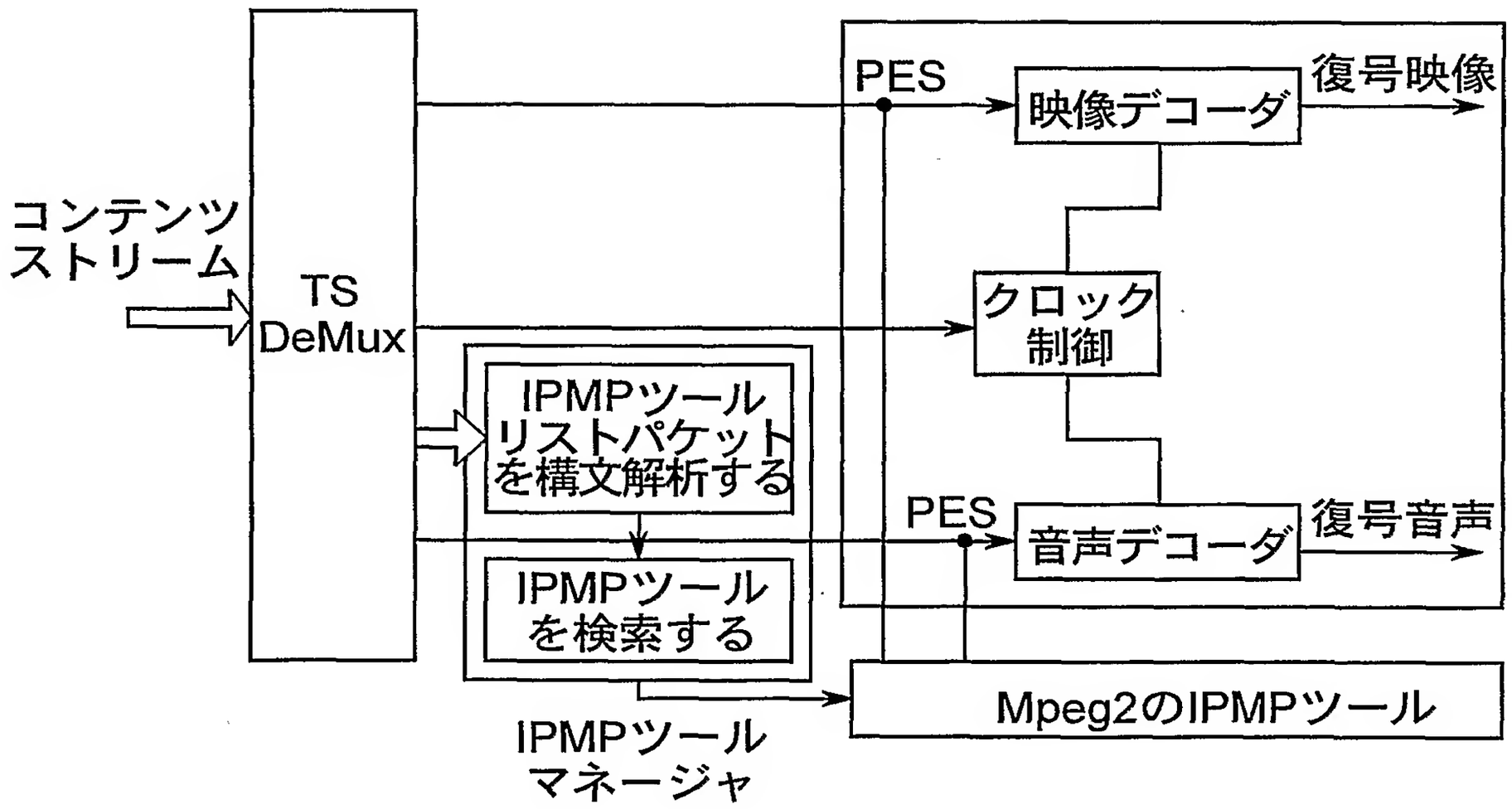


Fig.4

Fig.5



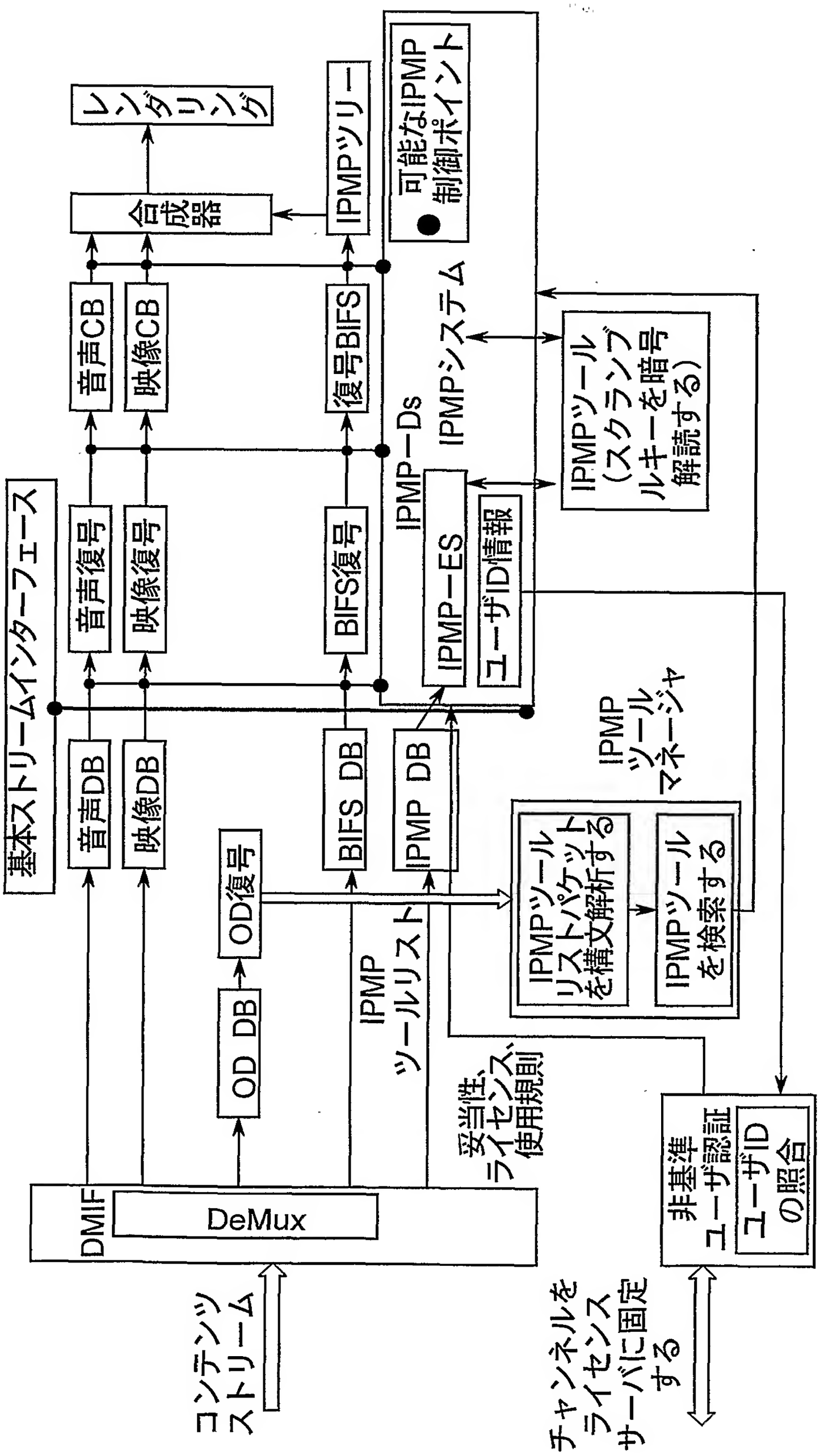


Fig.6

Fig.7

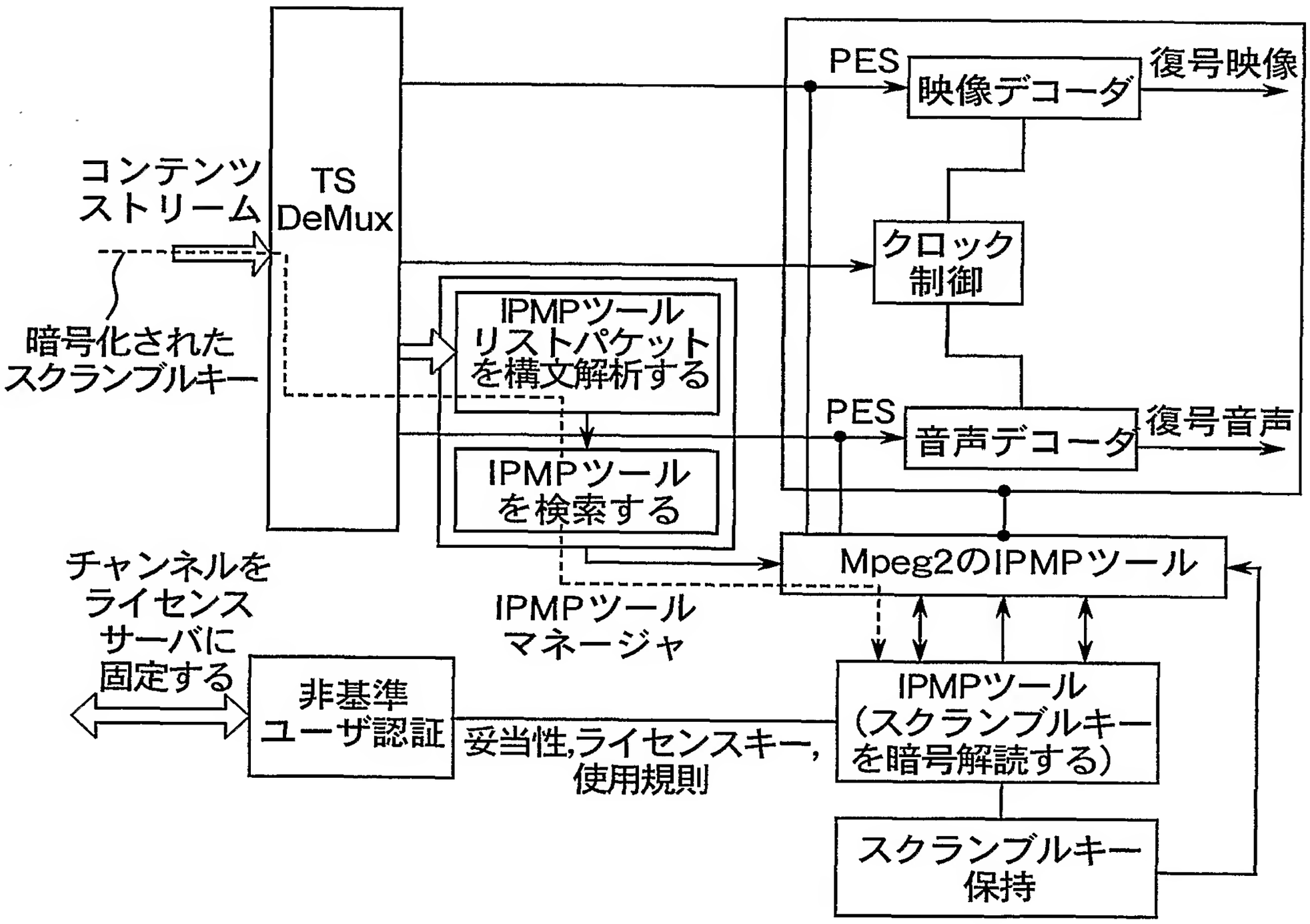


Fig.8

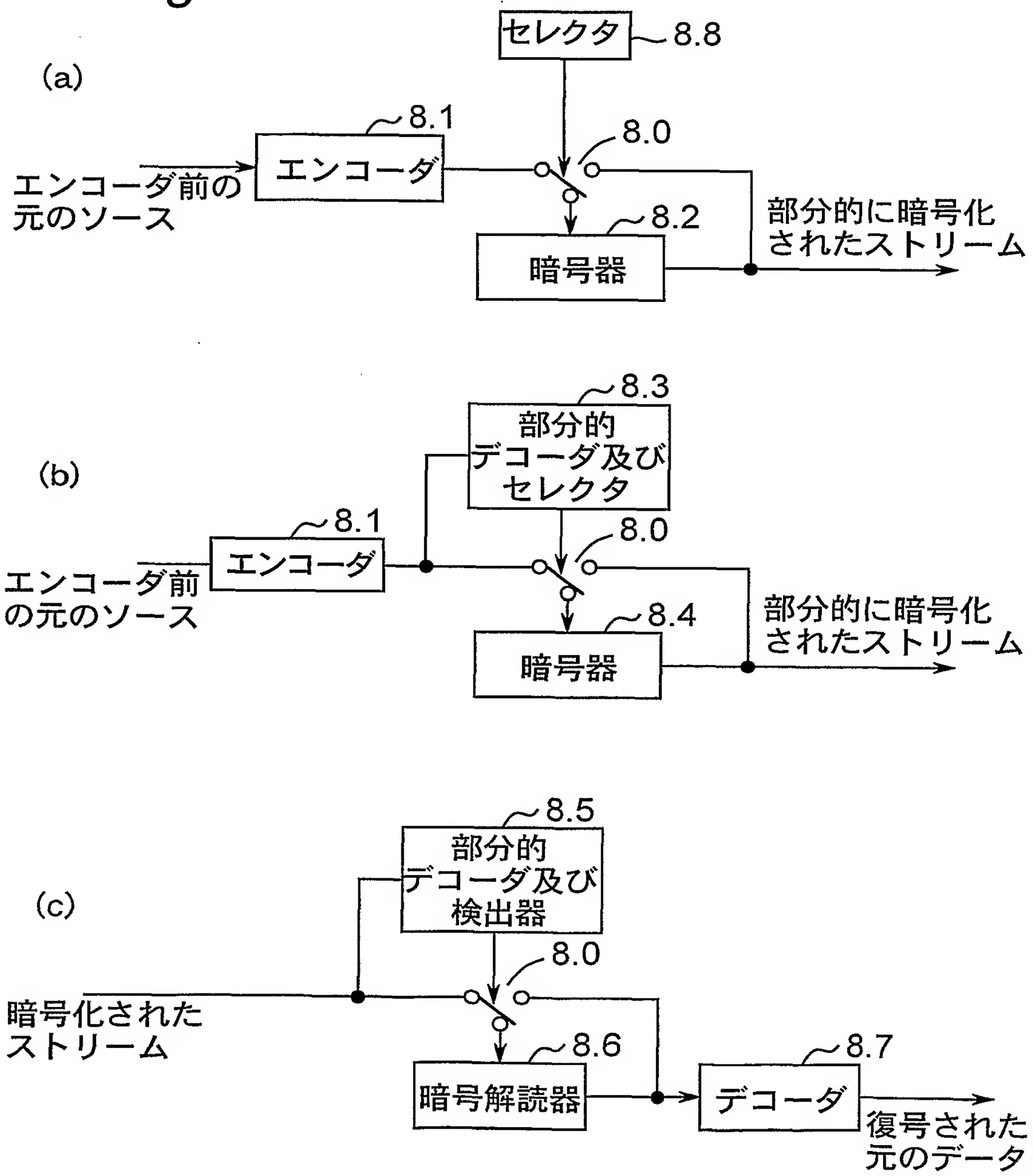


Fig.9

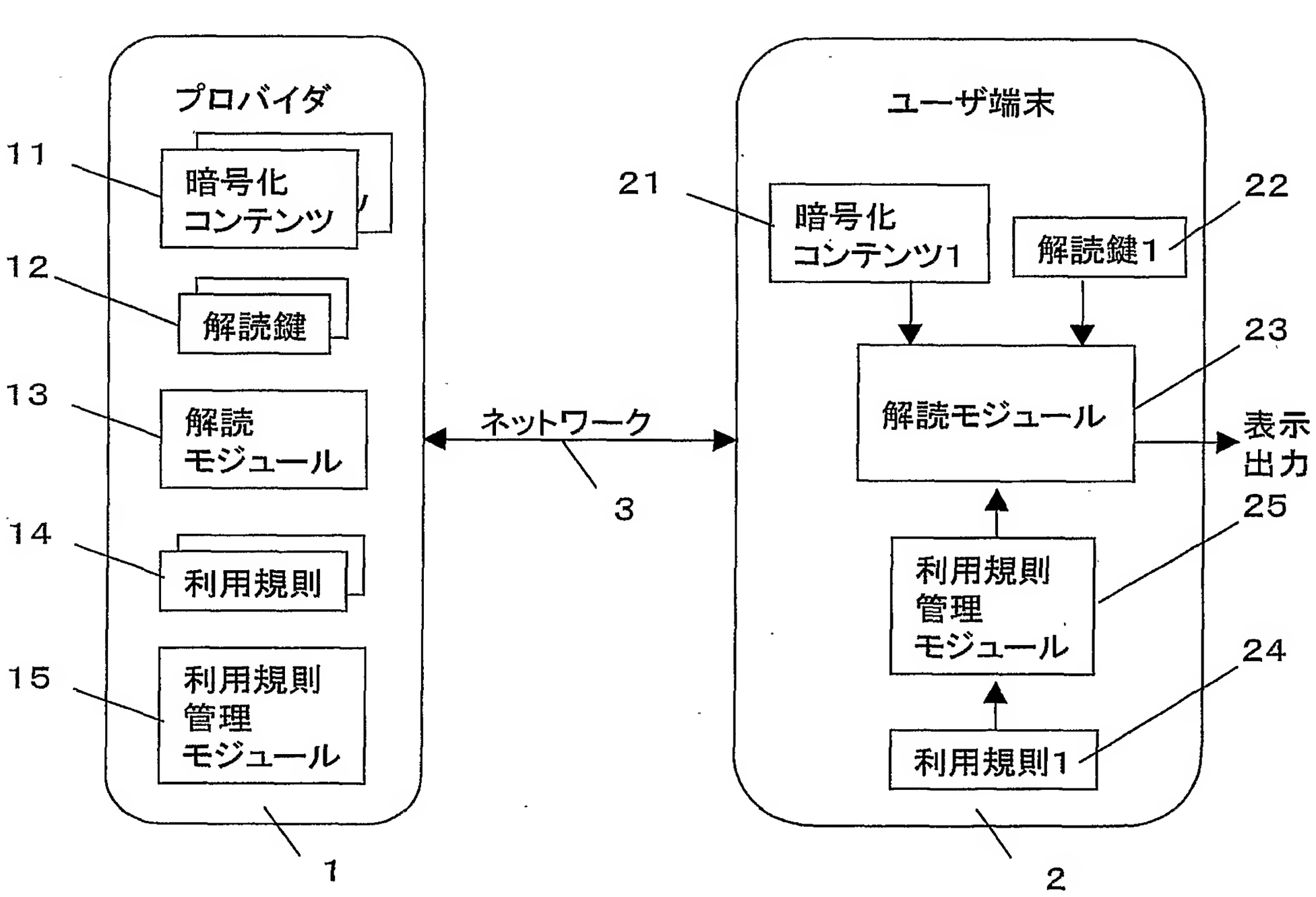


Fig.10

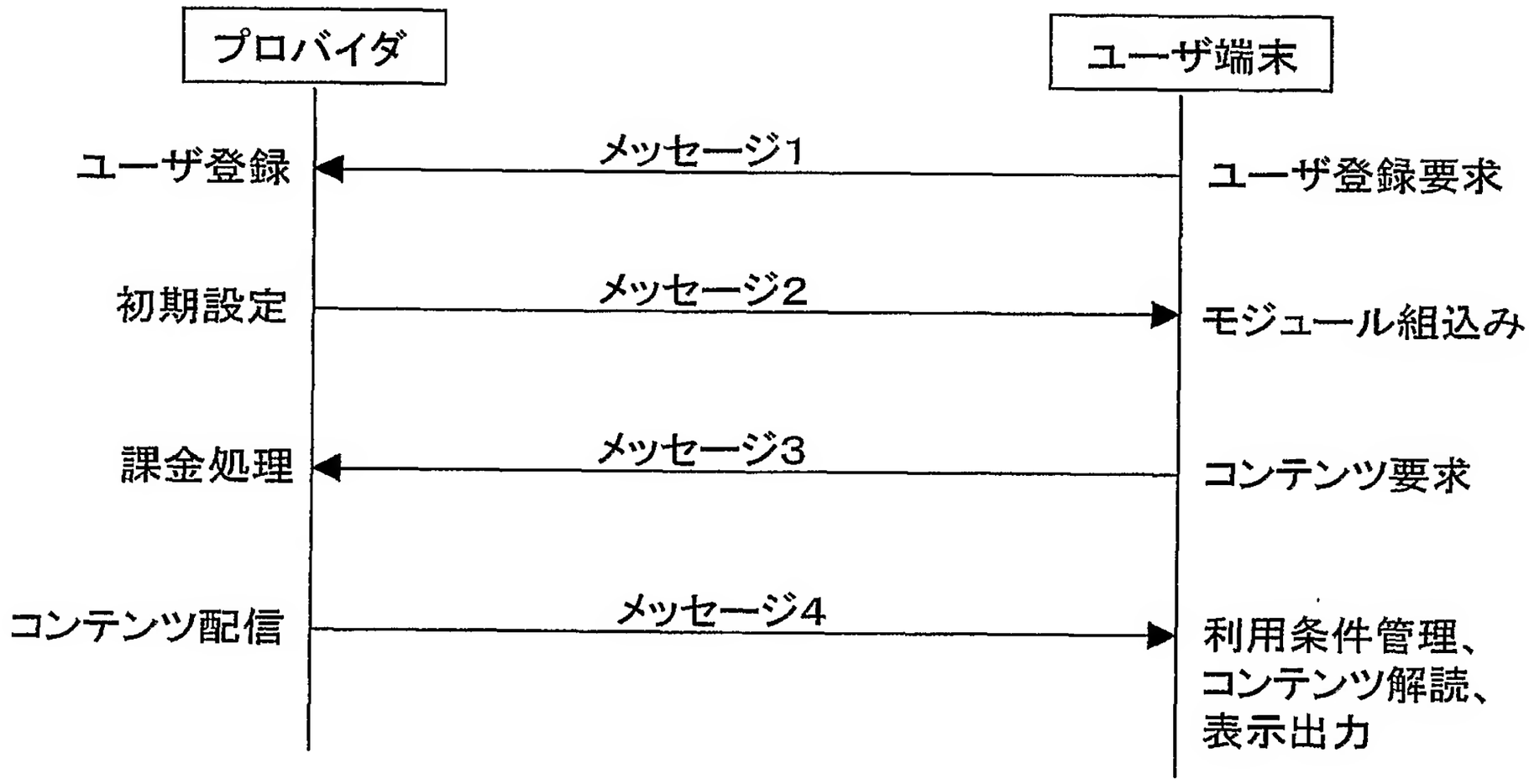


Fig.11

メッセージ1

メッセージID＝	ユーザ登録
ユーザ名＝	松下　太郎
支払い方法＝	クレジットカード番号
ユーザ端末情報＝	Windows OS

メッセージ2

メッセージID＝	初期設定
ユーザID＝	XYZ
IPMP情報=	コンテンツリスト
IPMPツール情報＝	解読モジュールID，ロケーション
IPMPツール情報＝	利用規則管理モジュールID，ロケーション

メッセージ3

メッセージID＝	コンテンツ要求
ユーザID＝	XYZ
コンテンツ情報=	コンテンツ1ID

メッセージ4

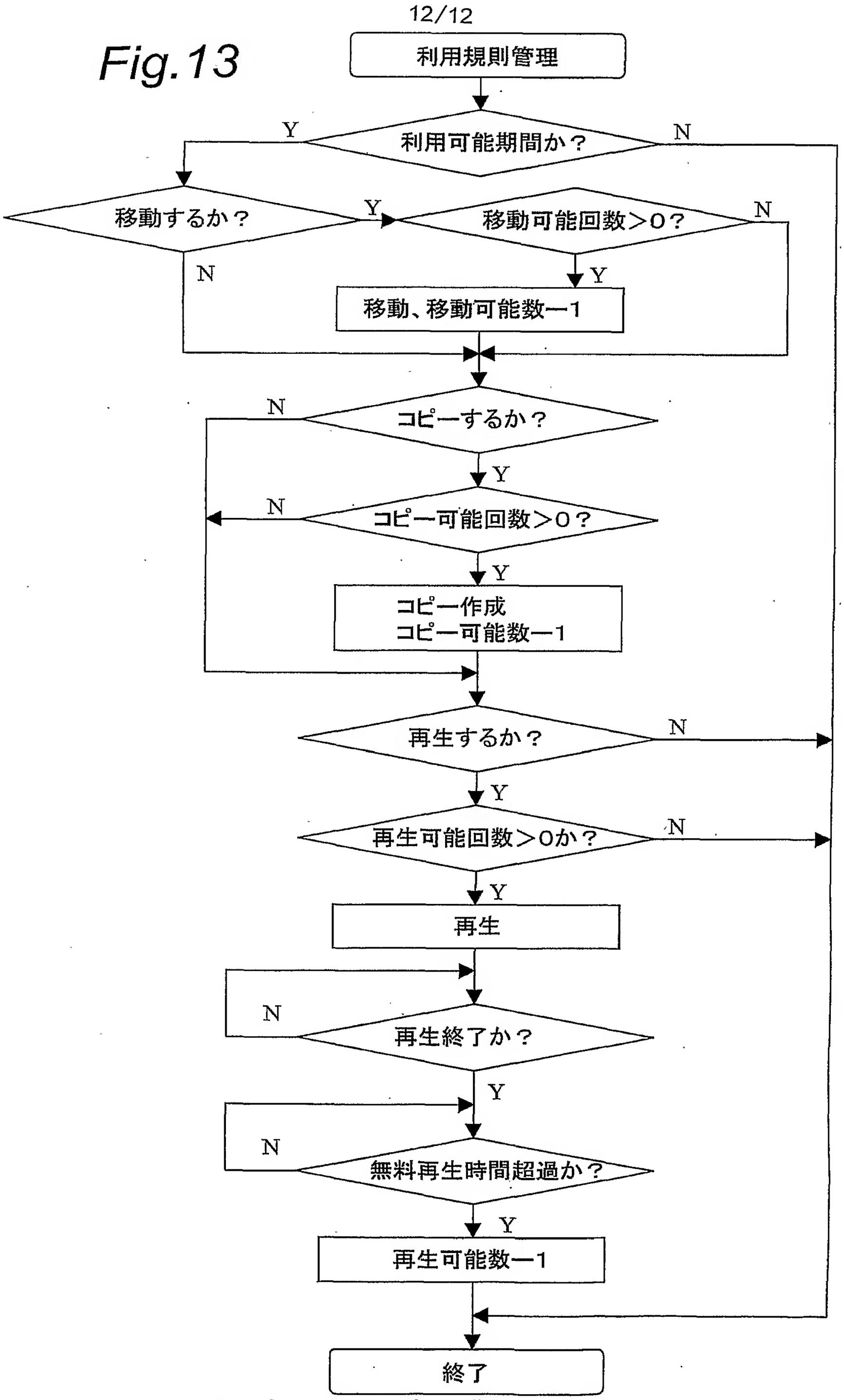
メッセージID＝	コンテンツ配信
IPMP情報＝	利用規則1
IPMP情報＝	解読鍵1
コンテンツ情報=	暗号化コンテンツ1

Fig.12

利用規則1

利用可能期間＝	2001.6.1-2001.6.30
無料再生時間＝	1分
再生可能回数＝	3
コピー可能回数＝	1
移動可能回数＝	5

Fig.13



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/05468

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/14, G06F17/60, G10L19/00, H04N7/08, H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/14, G06F17/60, G10L19/00, H04N7/08, H04N7/167

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2002
Kokai Jitsuyo Shinan Koho 1971-2002 Jitsuyo Shinan Toroku Koho 1996-2002

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST FILE(JOIS), WPI, INSPEC(DIALOG), IPMP

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	OPIMA Specification Version 1.1. [online], 27 June, 2000 (27.06.00), [retrieved on 2002-08-30]. Retreieved from the Internet:<URL:http://leonardo.telecomitalialab.com/opima/>, especially 2.4 Protocols, 3.3.3.2 getImpSystem	1-13,16-29, 31-35
Y	WO 99/48296A (INTERTRUST TECHNOLOGIES CORPORATION), 23 September, 1999 (23.09.99), Page 25, line 25 to page 26, line 14 & EP 1062812 A & CN 1301459 A & JP 2002-507868 A	1-13,16-29, 31-35
A	MPEG-4 Intellectual Property Management & Protection(IPMP) Overview & Applications. [online], 1998.12, [retrieved on 2002-08-30]. Retreieved from the Internet: <URL:http://mpeg.telecomitalialab.com/working_documents.htm>	1-13,16-29, 31-35

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 September, 2002 (12.09.02)	01 October, 2002 (01.10.02)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/05468

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Intellectual Property Management and Protection in MPEG Standards. [online], 2001.01, [retrieved on 2002-08-30]. Retreieved from the Internet:<URL:http://mpeg.telecomitalialab.com/standards/ipmp/>	1-13,16-29, 31-35
A	Tadashi KANEKO, "MPEG-4 Chosakuken Kanri · Shien Field no Tokucho", Information Processing Society of Japan Kenkyu Hokoku, 30 January, 1999 (30.01.99), Vol.99, No.11, pages 25 to 32	1-13,16-29, 31-35
A	Tadashi KANEKO, Ikuo KUDO, "MPEG-4 ni okeru Chosakuken Shikibetsu Kanri no Hyojun Doko ni tsuite", Information Processing Society of Japan Kenkyu Hokoku, 29 May, 1998 (29.05.98), Vol.98, No.52, pages 75 to 82	1-13,16-29, 31-35

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/05468

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:

because they relate to subject matter not required to be searched by this Authority, namely:

2. ☒ Claims Nos.: 14, 15, 30

because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

The claims 14, 15, and 30 are so unclear that no meaningful international search can be carried out.

3. ☐ Claims Nos.:

because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. Claims 1-4, 11-13, 16-19, 27-29
2. Claims 5-9, 20-24
3. Claims 10, 26
4. Claim 25
5. Claims 31-35

Claims 14, 15, and 30 fall in the Japanese Law Concerning International Applications, Etc. Pursuant to PCT, Article 8, Paragraph 2, Subparagraph 2 (PCT Article 17(2)) and no meaningful international search can be carried out. Accordingly, these claims are not included in any of the aforementioned groups of inventions.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０２／０５４６８

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ９／１４　Ｇ０６Ｆ１７／６０　Ｇ１０Ｌ１９／００　Ｈ０４Ｎ７／０８　Ｈ０４Ｎ７／１６７

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ９／１４　Ｇ０６Ｆ１７／６０　Ｇ１０Ｌ１９／００　Ｈ０４Ｎ７／０８　Ｈ０４Ｎ７／１６７

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００２年
日本国登録実用新案公報	１９９４－２００２年
日本国実用新案登録公報	１９９６－２００２年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

ＪＩＣＳＴファイル（ＪＯＩＳ），ＷＰＩ，ＩＮＳＰＥＣ（ＤＩＡＬＯＧ）
IPMP

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	OPIMA Specification Version 1.1. [online], 2000.06.27, [retrieved on 2002-08-30]. Retreieved from the Internet: <URL:http://leonardo.telecomitalialab.com/opima/>, especially 2.4 Protocols, 3.3.3.2 getImpSystem	1-13,16-29, 31-35
Y	WO 99/48296 A (INTERTRUST TECHNOLOGIES CORPORATION) 1999.09.23, 第25頁第25行－第26頁第14行 & EP 1062812 A & CN 1301459 A & JP 2002-507868 A	1-13,16-29, 31-35

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日　１２．０９．０２	国際調査報告の発送日　01.10.02
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｍ　９３６４ 中里　裕正 電話番号　０３－３５８１－１１０１　内線　３５９７

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	MPEG-4 Intellectual Property Management & Protection(IPMP) Overview & Applications. [online], 1998.12, [retrieved on 2002-08-30]. Retreieved from the Internet: <URL:http://mpeg.telecomitalialab.com/working_documents.htm>	1-13,16-29, 31-35
A	Intellectual Property Management and Protection in MPEG Standards. [online], 2001.01, [retrieved on 2002-08-30]. Retreieved from the Internet: <URL:http://mpeg.telecomitalialab.com/standards/ipmp/>	1-13,16-29, 31-35
A	金子格, ＭＰＥＧ－４著作権管理・支援フィールドの特徴, 情報処理学会研究報告, 1999.01.30, Vol.99, No.11, p.25-32	1-13,16-29, 31-35
A	金子格，工藤育男, ＭＰＥＧ－４における著作権識別管理の標準動向について, 情報処理学会研究報告, 1998.05.29, Vol.98, No.52, p.75-82	1-13,16-29, 31-35

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０２／０５４６８

第Ⅰ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

2．☒ 請求の範囲 １４，１５，３０ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
請求の範囲の記載が著しく不明確であるため、有効な国際調査をすることができない。

3．☐ 請求の範囲 _____ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅱ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

１．請求の範囲１－４，１１－１３，１６－１９，２７－２９
２．請求の範囲５－９，２０－２４
３．請求の範囲１０，２６
４．請求の範囲２５
５．請求の範囲３１－３５

請求の範囲１４，１５，３０は、法第８条第２項第２号に該当し（ＰＣＴ１７条(2)）、国際調査を行うことができないので、どの発明にも含まれていない。

1．☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☒ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意
☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。